Installations- und Einrichtungshandbuch für vSphere

Update 1

vSphere 6.0

Dieses Dokument unterstützt die aufgeführten Produktversionen sowie alle folgenden Versionen, bis das Dokument durch eine neue Auflage ersetzt wird. Die neuesten Versionen dieses Dokuments finden Sie unter
http://www.vmware.com/de/support/pubs.

DE-001784-00



Die neueste technische Dokumentation finden Sie auf der VMware-Website unter:

http://www.vmware.com/de/support/

Auf der VMware-Website finden Sie auch die aktuellen Produkt-Updates.

Falls Sie Anmerkungen zu dieser Dokumentation haben, senden Sie Ihre Kommentare und Vorschläge an:

docfeedback@vmware.com

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

VMware Global, Inc.
Zweigniederlassung Deutschland
Freisinger Str. 3
85716 Unterschleißheim/Lohhof
Germany
Tel.: +49 (0) 89 3706 17000
Fax: +49 (0) 89 3706 17333
www.vmware.com/de

Inhalt

Grundlegende Informationen zur Installation und Einrichtung von vSphere

vSphere-Installation und -Einrichtung beschreibt, wie Sie VMware® vCenter Server installieren und konfigurieren und die vCenter Server Appliance und ESXi bereitstellen.

Zielgruppe

vSphere-Installation und -Einrichtung richtet sich an erfahrene Administratoren, die vCenter Server installieren und konfigurieren, vCenter Server Appliance bereitstellen und konfigurieren und ESXi installieren und konfigurieren möchten.

Diese Informationen sind für erfahrene Systemadministratoren bestimmt, die mit der Windows- oder Linux-VM-Technologie und Datencenteroperationen vertraut sind. Die Informationen über die Verwendung von Image Builder und Auto Deploy wenden sich an Administratoren mit Erfahrung in Microsoft PowerShell und PowerCLI.

Einführung in Installation und Einrichtung von vSphere 1

vSphere 6.0 bietet mehrere Installations- und Setup-Optionen. Machen Sie sich mit den Installations- und Setup-Optionen sowie der Reihenfolge der Aufgaben vertraut, um für eine erfolgreiche vSphere-Bereitstellung zu sorgen.

Die zwei Hauptkomponenten von vSphere sind VMware ESXi® und VMware vCenter Server®. ESXi ist die Virtualisierungsplattform, auf der Sie virtuelle Maschinen und virtuelle Appliances erstellen und ausführen können. vCenter Server ist ein Dienst, der als zentraler Administrator für in einem Netzwerk miteinander verbundene ESXi-Hosts agiert. Mit vCenter Server können Sie die Ressourcen mehrerer Hosts in einem Pool zusammenfassen und verwalten.

Sie können vCenter Server auf einer virtuellen Windows-Maschine oder einem physischen Server installieren oder die vCenter Server Appliance bereitstellen. Die vCenter Server Appliance ist eine vorkonfigurierte Linux-basierte virtuelle Maschine, die für die Ausführung von vCenter Server und der vCenter Server-Komponenten optimiert ist. Die vCenter Server Appliance kann auf ESXi-Hosts der Version 5.0 oder höher oder auf vCenter Server-Instanzen der Version 5.0 oder höher bereitgestellt werden.

Ab vSphere 6.0 sind alle vorausgesetzten Dienste für die Ausführung von vCenter Server und der vCenter Server-Komponenten im VMware Platform Services Controller gebündelt. Sie können vCenter Server mit einem eingebetteten oder externen Platform Services Controller bereitstellen, aber Sie müssen immer den Platform Services Controller vor vCenter Server installieren bzw. bereitstellen.

Dieses Kapitel behandelt die folgenden Themen:

vCenter Server -Komponenten und -Dienste

vCenter Server bietet eine zentrale Plattform, um virtuelle Maschinen und Hosts zu verwalten und zu betreiben, um Ressourcen für sie bereitzustellen und ihre Leistung zu bewerten.

Wenn Sie vCenter Server mit eingebettetem Platform Services Controller installieren oder die vCenter Server Appliance mit einem eingebetteten Platform Services Controller bereitstellen, werden vCenter Server, die vCenter Server-Komponenten und die beim Platform Services Controller enthaltenen Dienste auf demselben System bereitgestellt.

Wenn Sie vCenter Server mit einem externen Platform Services Controller installieren oder die vCenter Server Appliance mit einem externen Platform Services Controller bereitstellen, werden vCenter Server und die vCenter Server-Komponenten auf einem bestimmten System und die beim Platform Services Controller enthaltenen Dienste auf einem anderen System bereitgestellt.

Die folgenden Komponenten sind in den Installationen von vCenter Server und vCenter Server Appliance enthalten:

- Die VMware Platform Services Controller-Gruppe von Infrastrukturdiensten beinhaltet vCenter Single Sign On, Lizenzdienst, Lookup Service und die VMware-Zertifizierungsstelle.
- Die vCenter Server-Gruppe von Diensten beinhaltet vCenter Server, vSphere Web Client, Inventory Service, vSphere Auto Deploy, vSphere ESXi Dump Collector, VMware vSphere Syslog Collector unter Windows und den VMware Syslog-Dienst für die vCenter Server Appliance.

Mit VMware Platform Services Controller installierte Dienste

vCenter Single Sign On

Der vCenter Single Sign On-Authentifizierungsdienst bietet sichere Authentifizierungsdienste für die vSphere-Softwarekomponenten. Bei Verwendung von vCenter Single Sign On kommunizieren die vSphere-Softwarekomponenten über einen sicheren Token-Austauschmechanismus miteinander, anstatt dass jede Komponente einen Benutzer über einen Verzeichnisdienst wie Active Directory separat authentifizieren muss. vCenter Single Sign On erstellt eine interne Sicherheitsdomäne (zum Beispiel „vsphere.local“), in der die vSphere-Lösungen und -Komponenten bei der Installation oder beim Upgrade registriert werden, wodurch eine Infrastrukturressource bereitgestellt wird. vCenter Single Sign On kann Benutzer über seine eigenen internen Benutzer und Gruppen authentifizieren oder eine Verbindung mit vertrauenswürdigen externen Verzeichnisdiensten wie Microsoft Active Directory herstellen. Authentifizierten Benutzern können dann registrierte lösungsbasierte Berechtigungen oder Rollen in einer vSphere-Umgebung zugewiesen werden.

vCenter Single Sign On ist für vCenter Server 5.1.x und höher verfügbar und erforderlich.

vSphere-Lizenzdienst

Der vSphere-Lizenzdienst stellt übliche Lizenzbestands- und -verwaltungsfunktionen für alle vCenter Server-Systeme bereit, die mit einem Platform Services Controller bzw. mehreren miteinander verknüpften Platform Services Controller-Instanzen verbunden sind.

VMware-Zertifizierungsstelle

Die VMware-Zertifizierungsstelle (VMCA) stellt für jeden ESXi-Host ein signiertes Zertifikat bereit, dessen Rootzertifizierungsstelle standardmäßig die VMCA ist. Diese Bereitstellung findet statt, wenn der ESXi-Host explizit oder im Zuge der Installation des ESXi-Hosts zu vCenter Server hinzugefügt wird. Alle ESXi-Zertifikate werden lokal auf dem Host gespeichert.

Mit vCenter Server installierte Dienste

Diese zusätzlichen Komponenten werden bei der Installation von vCenter Server automatisch installiert. Die Komponenten können nicht separat installiert werden, weil es keine eigenen Installationsprogramme dafür gibt.

vCenter Inventory Service
Inventory Service speichert vCenter Server-Konfigurations- und Bestandslistendaten. Somit können Sie Bestandslistenobjekte in vCenter Server-Instanzen durchsuchen und auf sie zugreifen.

PostgreSQL
Eine gebündelte Version der VMware-Verteilung der PostgreSQL-Datenbank für vSphere und vCloud Hybrid-Dienste.

vSphere Web Client
Über den vSphere Web Client können Sie mithilfe eines Webbrowsers eine Verbindung mit vCenter Server-Instanzen herstellen, um Ihre vSphere-Infrastruktur zu verwalten.

vSphere ESXi Dump Collector
Das vCenter Server-Support-Tool. ESXi kann so konfiguriert werden, dass der VMkernel-Arbeitsspeicher auf einem Netzwerkserver anstatt einer Festplatte gespeichert wird, wenn ein kritischer Fehler im System auftritt. Der vSphere ESXi-Dump Collector sammelt solche Speicher-Dumps im Netzwerk.

VMware vSphere Syslog Collector
Das Support-Tool von vCenter Server unter Windows, das die Netzwerkprotokollierung aktiviert und die Protokolle von mehreren Hosts kombiniert. Sie können mit dem vSphere Syslog Collector ESXi-Systemprotokolle an einen Server im Netzwerk statt an eine lokale Festplatte weiterleiten. Die empfohlene maximale Anzahl unterstützter Hosts, von denen Protokolle erfasst werden, beträgt 30. Informationen zum Konfigurieren von vSphere Syslog Collector finden Sie unter http://kb.vmware.com/kb/2021652.

VMware Syslog-Dienst
Das Support-Tool von vCenter Server Appliance, das eine einheitliche Architektur für die Systemprotokollierung, die Netzwerkprotokollierung und das Erfassen von Protokollen von mehreren Hosts bietet. Sie können mit dem VMware Syslog-Dienst ESXi-Systemprotokolle an einen Server im Netzwerk statt an eine lokale Festplatte weiterleiten. Die empfohlene maximale Anzahl unterstützter Hosts, von denen Protokolle erfasst werden, beträgt 30. Informationen zum Konfigurieren des VMware Syslog-Diensts finden Sie unter *vCenter Server Appliance-Konfiguration*.

vSphere Auto Deploy
Das vCenter Server-Support-Tool, das Hunderte von physischen Hosts mit ESXi-Software bereitstellen kann. Sie können angeben, welches Image bereitgestellt werden soll und welche Hosts mit dem Image bereitgestellt werden sollen. Optional können Sie die Hostprofile, die auf die Hosts angewendet werden sollen, und einen vCenter Server-Speicherort (Ordner oder Cluster) für jeden Host angeben.

Bereitstellungsmodelle für vCenter Server

Sie können vCenter Server auf einer virtuellen Maschine oder einem physischen Server unter Microsoft Windows Server 2008 SP2 oder höher installieren oder die vCenter Server Appliance bereitstellen. Die vCenter Server Appliance ist eine vorkonfigurierte Linux-basierte virtuelle Maschine, die für die Ausführung von vCenter Server optimiert ist.

vSphere 6.0 führt vCenter Server mit einem eingebetteten Platform Services Controller und vCenter Server mit einem externen Platform Services Controller ein.

Wichtig Diese Dokumentation enthält Informationen zu den grundlegenden Bereitstellungsmodellen. Informationen zu den empfohlenen Topologien finden Sie unter Aufstellung der empfohlenen Topologien für vSphere 6.0.x.

---

vCenter Server mit einem eingebetteten Platform Services Controller

Alle mit dem Platform Services Controller gebündelten Dienste werden auf derselben virtuellen Maschine oder demselben physischen Server wie vCenter Server bereitgestellt.

vCenter Server mit einem externen Platform Services Controller

Die mit dem Platform Services Controller und vCenter Server gebündelten Dienste werden auf verschiedenen virtuellen Maschinen oder physischen Servern bereitgestellt.

Sie müssen zuerst den Platform Services Controller auf einer virtuellen Maschine bzw. einem physischen Server und anschließend vCenter Server auf einer anderen virtuellen Maschine bzw. einem anderen physischen Server bereitstellen.

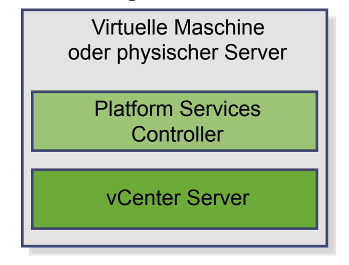
Hinweis Nach der Bereitstellung von vCenter Server mit eingebettetem Platform Services Controller können Sie Ihre Topologie neu konfigurieren und auf vCenter Server mit externem Platform Services Controller umstellen. Dieser Vorgang ist unumkehrbar und Sie können nicht wieder auf vCenter Server mit eingebettetem Platform Services Controller zurücksetzen. Die vCenter Server-Instanz können Sie nur auf einen externen Platform Services Controller neu verweisen, für den die Replizierung der Infrastrukturdaten innerhalb derselben Domäne konfiguriert ist.

---

vCenter Server mit einem eingebetteten Platform Services Controller

vCenter Server und der Platform Services Controller werden auf einer einzelnen virtuellen Maschine bzw. einem einzelnen physischen Server bereitgestellt.

Abbildung 1-1. vCenter Server mit eingebettetem Platform Services Controller



Das Installieren von vCenter Server mit einem eingebetteten Platform Services Controller hat die folgenden Vorteile:

- Die Verbindung zwischen vCenter Server und dem Platform Services Controller erfolgt nicht über das Netzwerk und vCenter Server ist nicht für Ausfälle wegen Verbindungs- und Namensauflösungsproblemen zwischen vCenter Server und dem Platform Services Controller anfällig.

- Wenn Sie vCenter Server auf virtuellen Windows-Maschinen oder physischen Servern installieren, benötigen Sie weniger Windows-Lizenzen.
- Sie brauchen weniger virtuelle Maschinen oder physische Server zu verwalten.
- Sie benötigen keinen Lastausgleichsdienst zum Verteilen der Last auf dem Platform Services Controller.

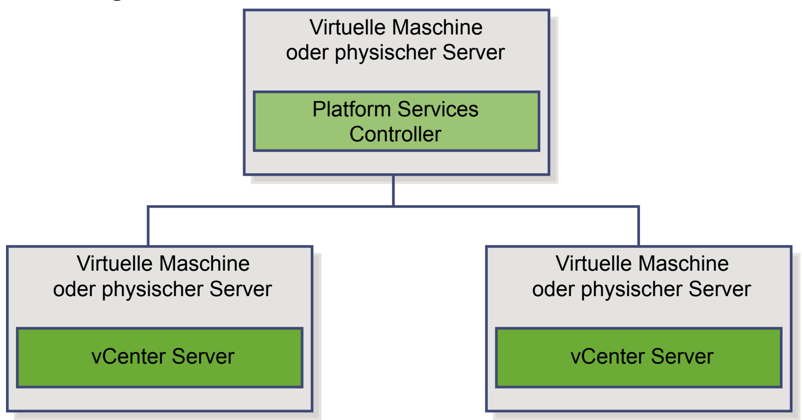
Die Installation mit einem eingebetteten Platform Services Controller hat die folgenden Nachteile:

- Es gibt einen Platform Services Controller für jedes Produkt, also möglicherweise mehr, als erforderlich sind. Dadurch werden mehr Ressourcen verbraucht.
- Das Modell ist für kleinere Umgebungen geeignet.

vCenter Server mit einem externen Platform Services Controller

vCenter Server und der Platform Services Controller werden auf einer separaten virtuellen Maschine bzw. einem separaten physischen Server bereitgestellt. Der Platform Services Controller kann in mehreren vCenter Server-Instanzen gleichzeitig verwendet werden. Sie können einen Platform Services Controller und dann mehrere vCenter Server-Instanzen installieren und diese dann beim Platform Services Controller registrieren. Sie können dann einen anderen Platform Services Controller installieren, ihn so konfigurieren, dass Daten vom ersten Platform Services Controller repliziert werden, und dann vCenter Server-Instanzen installieren und diese beim zweiten Platform Services Controller registrieren.

Abbildung 1-2. vCenter Server mit einem externen Platform Services Controller



Die Installation von vCenter Server mit einem externen Platform Services Controller hat die folgenden Vorteile:

- Ein geringerer Ressourcenverbrauch durch die kombinierten Dienste in den Platform Services Controller-Instanzen verringert den Speicherplatz- und Wartungsbedarf.
- Ihre Umgebung kann aus mehr vCenter Server-Instanzen bestehen.

Die Installation von vCenter Server mit einem externen Platform Services Controller hat die folgenden Nachteile:

- Die Verbindung zwischen vCenter Server und dem Platform Services Controller erfolgt über das Netzwerk und ist für Verbindungs- und Namensauflösungsprobleme anfällig.
- Wenn Sie vCenter Server auf virtuellen Windows-Maschinen oder physischen Servern installieren, benötigen Sie mehr Microsoft Windows-Lizenzen.
- Sie müssen mehr virtuelle Maschinen oder physische Server verwalten.

Umgebung mit gemischten Betriebssystemen

Eine unter Windows installierte vCenter Server-Instanz kann entweder bei einem unter Windows installierten Platform Services Controller oder einer Platform Services Controller-Appliance registriert werden. Eine vCenter Server Appliance kann entweder bei einem unter Windows installierten Platform Services Controller oder einer Platform Services Controller-Appliance registriert werden. Sowohl vCenter Server als auch die vCenter Server Appliance können bei demselben Platform Services Controller innerhalb einer Domäne registriert werden.

Abbildung 1-3. Beispiel einer Umgebung mit gemischten Betriebssystemen mit einem externen Platform Services Controller unter Windows

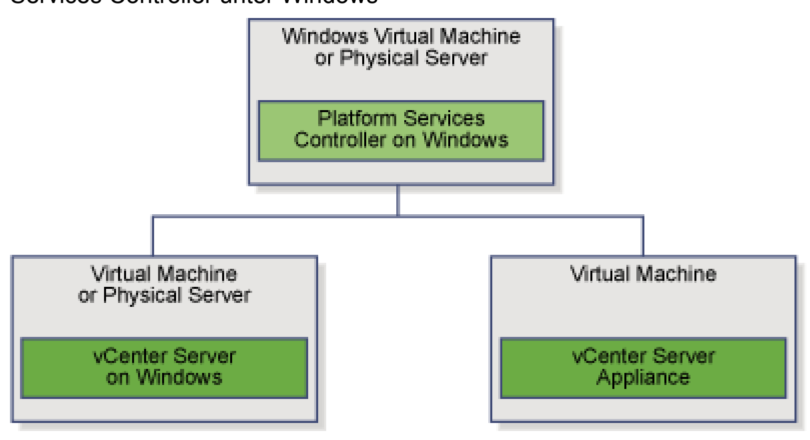
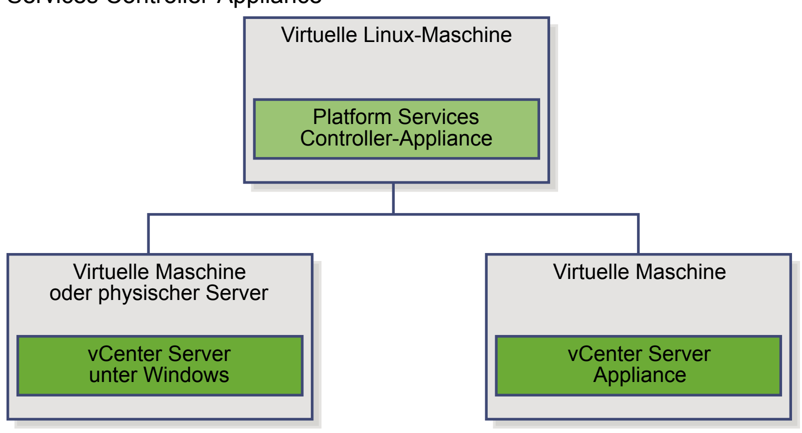


Abbildung 1-4. Beispiel einer Umgebung mit gemischten Betriebssystemen mit einer externen Platform Services Controller-Appliance



Mit vielen Platform Services Controller-Instanzen, die ihre Infrastrukturdaten replizieren, können Sie die Hochverfügbarkeit Ihres Systems sicherstellen.

Wenn ein externer Platform Services Controller, bei dem Ihre vCenter Server-Instanz oder vCenter Server Appliance anfangs registriert wurde, nicht mehr antwortet, können Sie Ihren vCenter Server oder die vCenter Server Appliance neu auf einen anderen externen Platform Services Controller in der Domäne verweisen. Weitere Informationen finden Sie unter „Neuverweisen der Verbindungen zwischen vCenter Server und Platform Services Controller“, auf Seite 280.

Übersicht über den vSphere-Installations- und Setup-Vorgang

vSphere ist ein ausgereiftes Produkt mit mehreren zu installierenden und einzurichtenden Komponenten. Machen Sie sich mit der Abfolge der Arbeitsschritte vertraut, um für eine erfolgreiche vSphere-Bereitstellung zu sorgen.

Die Installation von vSphere umfasst folgende Aufgaben:

1 Lesen Sie die vSphere-Versionshinweise.

2 Stellen Sie sicher, dass Ihr System die vSphere-Hardware- und Softwareanforderungen erfüllt. Siehe Kapitel 2, „Systemanforderungen“, auf Seite 21.

3 Installieren Sie ESXi.

   a Überprüfen Sie, ob Ihr System die Mindestanforderungen an die Hardware erfüllt. Siehe „Anforderungen für ESXi“, auf Seite 21.

   b Festlegen der zu verwendenden ESXi-Installationsoption. Siehe „Optionen für die Installation von ESXi“, auf Seite 39.

   c Legen Sie den Speicherort und die Startposition des ESXi-Installationsprogramms fest. Siehe „Medienoptionen für das Starten des ESXi-Installationsprogramms“, auf Seite 42. Wenn Sie das Installationsprogramm über PXE starten, überprüfen Sie, ob Ihre Netzwerk-PXE-Infrastruktur ordnungsgemäß eingerichtet ist. Siehe „Starten des ESXi-Installationsprogramms per PXE-Startvorgang“, auf Seite 46.

   d Erstellen Sie ein Arbeitsblatt mit den Informationen, die Sie für die Installation von ESXi benötigen. Siehe „Erforderliche Informationen für die Installation von ESXi“, auf Seite 55.

   e Installieren Sie ESXi.

   - „Interaktives Installieren von ESXi“, auf Seite 57
   - „Installieren oder Upgraden von Hosts mithilfe eines Skripts“, auf Seite 60
   - „Installieren von ESXi mithilfe von vSphere Auto Deploy“, auf Seite 76

   Wichtig In vSphere 6.0 wird Auto Deploy zusammen mit vCenter Server installiert. Zum Bereitstellen von ESXi-Hosts mithilfe von Auto Deploy müssen Sie vCenter Server installieren oder die vCenter Server Appliance bereitstellen.

4 Konfigurieren der ESXi-Start- und Netzwerkeinstellungen, der direkten Konsole und anderen Einstellungen. Siehe Kapitel 5, „Einrichten von ESXi“, auf Seite 177 und Kapitel 6, „Nach der Installation und Einrichtung von ESXi“, auf Seite 201.

5 Ziehen Sie es in Erwägung, einen Syslog-Server für die Remoteprotokollierung einzurichten, um ausreichend Speicherplatz für Protokolldateien zu gewährleisten. Die Einrichtung der Protokollierung auf einem Remotehost ist besonders wichtig für Hosts, die über begrenzten lokalen Speicher verfügen. Siehe „Erforderlicher freier Speicherplatz für die Systemprotokollierung“, auf Seite 38 und „Konfiguration von Syslog auf ESXi-Hosts“, auf Seite 195.

6 Installieren Sie vCenter Server auf einer virtuellen Windows-Maschine oder einem physischen Server oder stellen Sie die vCenter Server Appliance bereit.

   In vSphere 6.0 können Sie vCenter Server installieren oder die vCenter Server Appliance bereitstellen und im erweiterten verknüpften Modus durch Registrieren der vCenter Server-Instanz und der vCenter Server Appliance bei Platform Services Controller-Instanzen, die ihre Infrastrukturdaten replizieren, miteinander verbinden.

Parallele Installationen werden nicht unterstützt. Nach dem Installieren oder Bereitstellen eines Platform Services Controller müssen Sie vCenter Server-Instanzen bzw. die vCenter Server Appliance nacheinander installieren bzw. bereitstellen.

- Installieren Sie vCenter Server auf einer virtuellen Windows-Maschine oder einem physischen Server.

  1. Stellen Sie sicher, dass Ihr System die Hardware- und Softwareanforderungen für die Installation von vCenter Server erfüllt. Siehe „Anforderungen für vCenter Server für Windows“, auf Seite 27.
  2. (Optional) Richten Sie eine externe vCenter Server-Datenbank ein. Siehe „Vorbereiten der vCenter Server-Datenbanken“, auf Seite 205.

     Für eine Umgebung mit bis zu 20 Hosts und bis zu 200 virtuellen Maschinen können Sie die mitgelieferte PostgreSQL-Datenbank verwenden. Richten Sie für Produktions- und große Umgebungen eine externe Datenbank ein, weil die Migration von einer eingebetteten PostgreSQL-Datenbank zu einer externen Datenbank kein trivialer manueller Vorgang ist.
  3. Erstellen Sie ein Arbeitsblatt mit den Informationen, die Sie für die Installation benötigen. Siehe „Erforderliche Informationen für die Installation von vCenter Server“, auf Seite 232.
  4. Installieren Sie vCenter Server und den Platform Services Controller. Siehe Kapitel 8, „Installieren von vCenter Server auf einer virtuellen Windows-Maschine oder einem physischen Server“, auf Seite 247.

     Sie können vCenter Server mit einem eingebetteten oder externen Platform Services Controller installieren.

     Die Bereitstellung von vCenter Server mit einem eingebetteten Platform Services Controller ist für kleinere Umgebungen geeignet. Die Bereitstellung von vCenter Server mit einem externen Platform Services Controller ist für Umgebungen mit mehreren vCenter Server-Instanzen geeignet. Siehe „Bereitstellungsmodelle für vCenter Server“, auf Seite 12.

- Stellen Sie vCenter Server Appliance bereit.

  1. Lesen Sie die Themen unter „Anforderungen für die vCenter Server Appliance“, auf Seite 30 und stellen Sie sicher, dass Ihr System die Hardware- und Softwareanforderungen für die Bereitstellung der vCenter Server Appliance erfüllt.
  2. (Optional) Richten Sie eine externe Oracle-Datenbank ein. Die vCenter Server Appliance unterstützt nur eine Oracle-Datenbank als externe Datenbank. Siehe „Vorbereiten der vCenter Server-Datenbanken“, auf Seite 205.

     Sie können auch die mitgelieferte PostgreSQL-Datenbank verwenden, die für Umgebungen mit bis zu 1.000 Hosts und bis zu 10.000 virtuellen Maschinen geeignet ist.
  3. Lesen Sie unter „Erforderliche Informationen für die Bereitstellung der vCenter Server Appliance“, auf Seite 237 nach, um ein Arbeitsblatt mit den Informationen zu erstellen, die Sie für die Installation benötigen.
  4. Stellen Sie die vCenter Server Appliance mit einem eingebetteten Platform Services Controller oder mit einem externen Platform Services Controller bereit. Siehe Kapitel 9, „Bereitstellen der vCenter Server Appliance“, auf Seite 259.

     Die Bereitstellung von vCenter Server mit einem eingebetteten Platform Services Controller ist für kleinere Umgebungen geeignet. Die Bereitstellung von vCenter Server mit einem externen Platform Services Controller ist für Umgebungen mit mehreren vCenter Server-Instanzen geeignet. Siehe „Bereitstellungsmodelle für vCenter Server“, auf Seite 12.

7. Stellen Sie eine Verbindung mit vCenter Server über den vSphere Web Client her. Siehe Kapitel 11, „Nach der Installation des vCenter Server oder der Bereitstellung der vCenter Server Appliance“, auf Seite 277.

8 Konfigurieren Sie vCenter Server und die vCenter Server Appliance. Siehe *vCenter Server und Hostverwaltung* und *vCenter Server Appliance-Konfiguration*.

Übersicht über vSphere-Sicherheitszertifikate

ESXi-Hosts und vCenter Server kommunizieren auf sichere Weise über SSL, um Vertraulichkeit, Integrität der Daten und Authentifizierung zu gewährleisten.

In vSphere 6.0 stellt die VMware-Zertifizierungsstelle (VMCA) für jeden ESXi-Host ein signiertes Zertifikat bereit, dessen Rootzertifizierungsstelle standardmäßig die VMCA ist. Diese Bereitstellung findet statt, wenn der ESXi-Host explizit oder als Teil der Installation des ESXi-Hosts zu vCenter Server hinzugefügt wird. Alle ESXi-Zertifikate werden lokal auf dem Host gespeichert.

Sie können auch benutzerdefinierte Zertifikate mit einer anderen Root-Zertifizierungsstelle (CA) verwenden. Informationen zum Verwalten von Zertifikaten für ESXi-Hosts finden Sie in der Dokumentation *vSphere-Sicherheit*.

Alle Zertifikate für vCenter Server und die vCenter Server-Dienste werden im VMware-Zertifikatsspeicher (VMware Endpoint Certificate Store, VECS) gespeichert.

Sie können das VMCA-Zertifikat für vCenter Server durch ein anderes von einer Zertifizierungsstelle signiertes Zertifikat ersetzen. Wenn Sie ein Drittanbieterzertifikat verwenden möchten, installieren Sie den Platform Services Controller, fügen Sie VMCA das neue von einer Zertifizierungsstelle signierte Rootzertifikat hinzu und installieren Sie dann vCenter Server. Informationen zum Verwalten von vCenter Server-Zertifikaten finden Sie in der Dokumentation *vSphere-Sicherheit*.

Übersicht Zertifikatsersetzung

Sie können je nach der Unternehmensrichtlinie und den Anforderungen für das System, das Sie konfigurieren, verschiedene Arten von Zertifikatsersetzungen ausführen. Sie können jede Ersetzung mit dem Dienstprogramm „vSphere Certificate Manager“ oder manuell über die Befehlszeilenschnittstellen durchführen, die Teil Ihrer Installation sind.

VMCA ist in jedem Platform Services Controller und in jeder eingebetteten Bereitstellung enthalten. VMCA stellt jedem Knoten, jedem vCenter Server-Lösungsbenutzer und jedem ESXi-Host ein Zertifikat zur Verfügung, das von VMCA als Zertifizierungsstelle signiert wurde. vCenter Server-Lösungsbenutzer sind Gruppen von vCenter Server-Diensten. Eine Liste der Lösungsbenutzer finden Sie unter *vSphere-Sicherheit*.

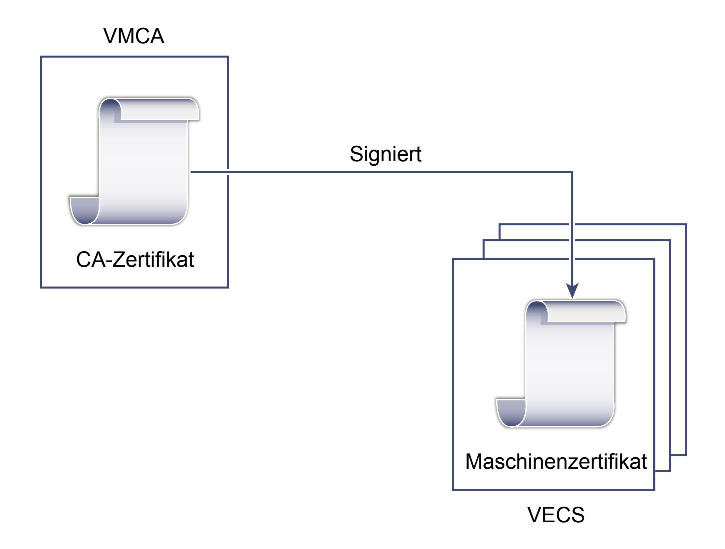
Sie können die Standardzertifikate ersetzen. Für vCenter Server-Komponenten können Sie einen Satz von Befehlszeilen-Tools verwenden, die bei Ihrer Installation enthalten sind. Es sind mehrere Optionen verfügbar.

Die Dokumentation *vSphere-Sicherheit* enthält ausführliche Informationen zu Ersetzungs-Workflows und zum Dienstprogramm „vSphere Certificate Manager“.

Ersetzen durch von VMCA signierte Zertifikate

Wenn Ihr VMCA-Zertifikat abläuft oder wenn Sie es aus anderen Gründen ersetzen möchten, können Sie dazu die Befehlszeilenschnittstellen zur Zertifikatsverwaltung verwenden. Standardmäßig läuft das VMCA-Rootzertifikat nach zehn Jahren ab, und alle von VMCA signierten Zertifikate laufen gleichzeitig mit dem Rootzertifikat ab, also nach maximal zehn Jahren.

Abbildung 1-5. Von VMCA signierte Zertifikate werden in VECS gespeichert

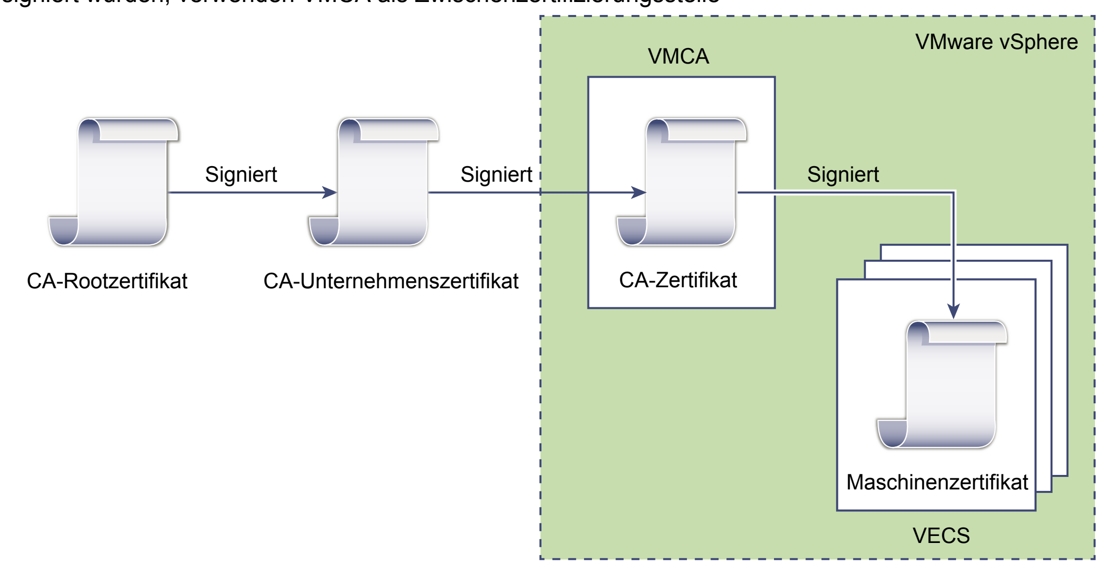


VMCA zu einer Zwischenzertifizierungsstelle machen

Sie können das VMCA-Rootzertifikat durch ein Zertifikat ersetzen, das durch eine Zertifizierungsstelle eines Unternehmens oder Drittanbieters signiert wurde. Die VMCA signiert das benutzerdefinierte Rootzertifikat immer, wenn sie Zertifikate zur Verfügung stellt, und macht so aus der VMCA eine Zwischenzertifizierungsstelle.

Hinweis Wenn Sie eine Neuinstallation mit einem externen Platform Services Controller durchführen, installieren Sie den Platform Services Controller zuerst und ersetzen Sie das VMCA-Rootzertifikat. Installieren Sie dann andere Dienste oder fügen Sie Ihrer Umgebung ESXi-Hosts hinzu. Wenn Sie eine Neuinstallation mit einem eingebetteten Platform Services Controller durchführen, ersetzen Sie das VMCA-Rootzertifikat vor dem Hinzufügen von ESXi-Hosts. In diesem Fall werden alle Zertifikate durch die ganze Kette signiert und Sie brauchen nicht neue Zertifikate zu generieren.

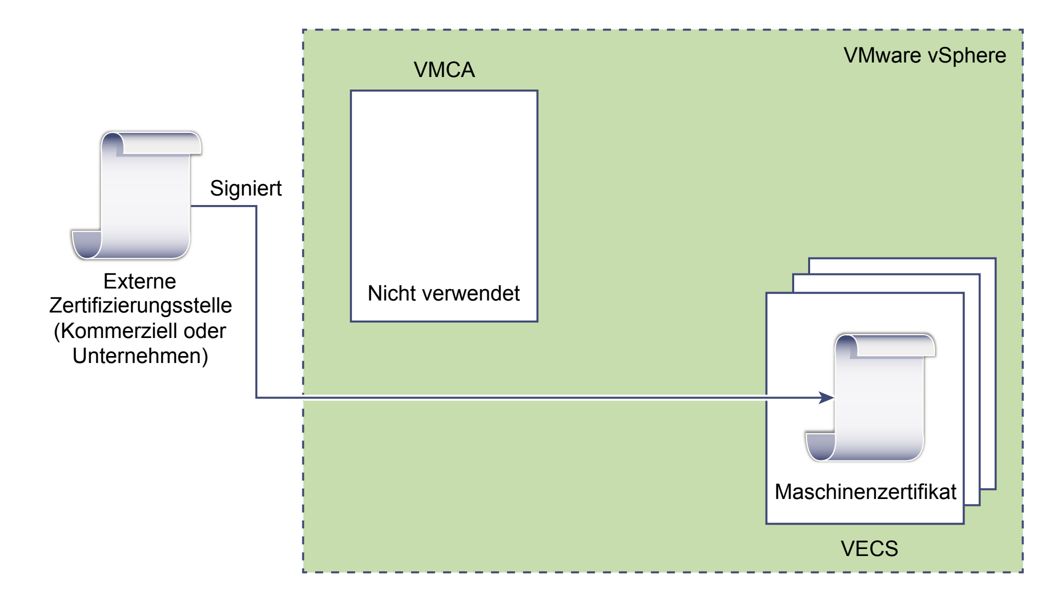
Abbildung 1-6. Zertifikate, die durch eine Zertifizierungsstelle eines Drittanbieters oder Unternehmens signiert wurden, verwenden VMCA als Zwischenzertifizierungsstelle



VMCA nicht verwenden, benutzerdefinierte Zertifikate zur Verfügung stellen

Sie können die vorhandenen VMCA-signierten Zertifikate durch benutzerdefinierte Zertifikate ersetzen. In diesem Fall sind Sie für die Bereitstellung und Überwachung aller Zertifikate verantwortlich.

Abbildung 1-7. Externe Zertifikate werden direkt in VECS gespeichert



Hybrid-Bereitstellung

Sie können für bestimmte Teile Ihrer Infrastruktur VMCA-Zertifikate und für andere Teile Ihrer Infrastruktur benutzerdefinierte Zertifikate verwenden. Beispiel: Weil Lösungsbenutzerzertifikate nur zum Authentifizieren bei vCenter Single Sign On verwendet werden, empfiehlt es sich, diese Zertifikate durch VMCA bereitstellen zu lassen. Ersetzen Sie die Maschinen-SSL-Zertifikate durch benutzerdefinierte Zertifikate, um den ganzen SSL-Datenverkehr abzusichern.

ESXi -Zertifikatsersetzung

Für ESXi-Hosts können Sie die Methode der Zertifikatsbereitstellung über den vSphere Web Client ändern.

Modus „VMware-Zertifizierungsstelle“ (Standard)
Wenn Sie Zertifikate über den vSphere Web Client erneuern, gibt VMCA die Zertifikate für die Hosts aus. Wenn Sie das VMCA-Rootzertifikat geändert haben, sodass eine Zertifikatskette enthalten ist, enthalten die Hostzertifikate die vollständige Kette.

Modus „Benutzerdefinierte Zertifizierungsstelle“
Damit können Sie Zertifikate, die nicht von VMCA signiert oder ausgegeben wurden, manuell aktualisieren und verwenden.

Fingerabdruckmodus
Kann verwendet werden, um 5.5-Zertifikate beim Aktualisieren beizubehalten. Verwenden Sie diesen Modus nur vorübergehend in Debugging-Situationen.

Erweiterter verknüpfter Modus – Überblick

Mit dem erweiterten verknüpften Modus werden mehrere vCenter Server-Systeme mithilfe von einer oder mehreren Platform Services Controller-Instanzen miteinander verbunden.

Mit dem erweiterten verknüpften Modus können Sie alle verknüpften vCenter Server-Systeme anzeigen und durchsuchen sowie Rollen, Berechtigungen, Lizenzen, Richtlinien und Tags replizieren.

Bei der Installation von vCenter Server oder der Bereitstellung der vCenter Server Appliance mit einem externen Platform Services Controller müssen Sie zunächst den Platform Services Controller installieren. Während der Installation des Platform Services Controller können Sie wählen, ob Sie eine neue vCenter Single Sign On-Domäne erstellen oder einer vorhandenen Domäne beitreten möchten. Sie können einer vorhandenen vCenter Single Sign On-Domäne beitreten, wenn Sie einen Platform Services Controller schon installiert oder bereitgestellt und eine vCenter Single Sign On-Domäne erstellt haben. Wenn Sie einer vorhandenen vCenter Single Sign On-Domäne beitreten, werden die Daten zwischen dem vorhandenen Platform Services Controller und dem neuen Platform Services Controller repliziert, und die Infrastrukturdaten werden zwischen den zwei Platform Services Controller-Instanzen ebenfalls repliziert.

Mit dem erweiterten verknüpften Modus können Sie nicht nur vCenter Server-Systeme unter Windows, sondern auch viele vCenter Server Appliance-Instanzen miteinander verbinden. Sie können außerdem eine Umgebung einrichten, in der mehrere vCenter Server-Systeme und vCenter Server Appliance-Instanzen miteinander verknüpft sind.

Wenn Sie vCenter Server mit einem externen Platform Services Controller installieren, müssen Sie zuerst den Platform Services Controller auf einer virtuellen Maschine bzw. einem physischen Server und anschließend vCenter Server auf einer anderen virtuellen Maschine bzw. einem anderen physischen Server bereitstellen. Beim Installieren von vCenter Server müssen Sie den externen Platform Services Controller auswählen. Stellen Sie sicher, dass der Platform Services Controller, den Sie auswählen, ein externer eigenständiger Platform Services Controller ist. Die Auswahl eines vorhandenen Platform Services Controller, der Teil einer eingebetteten Installation ist, wird nicht unterstützt und dies kann nach der Bereitstellung nicht neu konfiguriert werden. Informationen zu den empfohlenen Topologien finden Sie unter http://kb.vmware.com/kb/2108548.

Systemanforderungen 2

Systeme, auf denen vCenter Server unter Windows, die vCenter Server Appliance und ESXi-Instanzen ausgeführt werden, müssen bestimmte Hardware- und Betriebssystemanforderungen erfüllen.

Wenn Sie Auto Deploy zum Bereitstellen von ESXi-Hosts verwenden, lesen Sie auch „Vorbereitung für vSphere Auto Deploy“, auf Seite 87.

Dieses Kapitel behandelt die folgenden Themen:

Anforderungen für ESXi

Für die Installation von ESXi oder das Upgrade auf ESXi 6.0 muss Ihr System bestimmte Hardware- und Softwareanforderungen erfüllen.

Hardwareanforderungen für ESXi

Stellen Sie sicher, dass der Host die Mindestanforderungen an die Hardwarekonfiguration erfüllt, die von ESXi 6.0 unterstützt werden.

Hardware- und Systemressourcen

Für die Installation bzw. das Upgrade von ESXi 6.0 müssen Ihre Hardware- und Systemressourcen die folgenden Anforderungen erfüllen:

- Unterstützte Serverplattform. Eine Liste der unterstützten Plattformen finden Sie im *VMware-Kompatibilitätshandbuch* unter http://www.vmware.com/resources/compatibility.
- Für ESXi 6.0 ist eine Hostmaschine mit mindestens zwei CPU-Kernen erforderlich.

- ESXi 6.0 unterstützt 64-Bit-x86-Prozessoren, die nach September 2006 veröffentlicht wurden. Hierzu zählt ein breites Spektrum von Prozessoren mit mehreren Kernen. Eine vollständige Liste der unterstützten Prozessoren finden Sie im VMware-Kompatibilitätshandbuch unter http://www.vmware.com/resources/compatibility.
- Für ESXi 6.0 muss das NX/XD-Bit für die CPU im BIOS aktiviert sein.
- ESXi benötigt mindestens 4 GB an physischem Arbeitsspeicher. Es wird empfohlen, mindestens 8 GB RAM zum Ausführen virtueller Maschinen in typischen Produktionsumgebungen bereitzustellen.
- Um virtuelle 64-Bit-Maschinen zu unterstützen, muss auf x64-CPUs die Unterstützung für die Hardwarevirtualisierung (Intel VT-x oder AMD RVI) aktiviert sein.
- Ein oder mehr Gigabit oder schnellere Ethernet-Controller. Eine Liste mit unterstützten Netzwerkadaptermodellen finden Sie im *VMware-Kompatibilitätshandbuch* unter http://www.vmware.com/resources/compatibility.
- SCSI-Festplatte oder lokale (nicht im Netzwerk befindliche) RAID-LUN mit nicht partitioniertem Bereich für die virtuelle Maschinen.
- Serial ATA (SATA) – eine über unterstützte SAS-Controller oder unterstützte On-Board-SATA-Controller verbundene Festplatte. SATA-Festplatten werden als remote betrachtet, nicht lokal. Diese Festplatten werden nicht standardmäßig als Scratch-Partition verwendet, da sie als remote betrachtet werden.

  Hinweis Sie können auf einem ESXi 6.0-Host kein SATA-CD-ROM-Gerät mit einer virtuellen Maschine verbinden. Zur Verwendung des SATA-CD-ROM-Laufwerks müssen Sie den IDE-Emulationsmodus einsetzen.

Speichersysteme

Eine Liste aller unterstützten Speichersysteme finden Sie im *VMware-Kompatibilitätshandbuch* unter http://www.vmware.com/resources/compatibility. Informationen zu Software-Fibre-Channel über Ethernet (FCoE) finden Sie unter „Installieren und Starten von ESXi mit Software FCoE“, auf Seite 54.

Startanforderungen für ESXi

vSphere 6.0 unterstützt das Starten von ESXi-Hosts von der Unified Extensible Firmware Interface (UEFI) aus. Mithilfe von UEFI können Sie Systeme von Festplatten, CD-ROM-Laufwerken oder USB-Medien aus starten. Das Starten oder Bereitstellen über das Netzwerk mit VMware Auto Deploy erfordert die Legacy-BIOS-Firmware und steht mit UEFI nicht zur Verfügung.

ESXi kann von einer Festplatte größer als 2 TB starten, vorausgesetzt, dass die System-Firmware und die Firmware auf allen von Ihnen verwendeten Erweiterungskarten unterstützt werden. Informationen finden Sie in der Dokumentation des Anbieters.

Hinweis Das Ändern des Boot-Typs von Legacy-BIOS in UEFI, nachdem Sie ESXi 6.0 installiert haben, kann dazu führen, dass der Host nicht gestartet werden kann. In diesem Fall zeigt der Host eine Fehlermeldung ähnlich der folgenden an: `Keine VMware-Startbank`. Das Ändern des Host-Boot-Typs zwischen Legacy-BIOS und UEFI wird nicht unterstützt, nachdem Sie ESXi 6.0 installiert haben.

Speicheranforderungen für die Installation von ESXi 6.0 bzw. das Upgrade auf ESXi 6.0

Zum Installieren von ESXi 6.0 bzw. das Upgrade auf ESXi 6.0 ist ein Startgerät mit mindestens 1 GB Speicherplatz erforderlich. Beim Starten von einer lokalen Festplatte oder einer SAN/iSCSI LUN ist eine 5,2-GB-Festplatte erforderlich, damit das VMFS-Volume und eine 4-GB-Scratch-Partition auf dem Startgerät erstellt werden können. Wenn eine kleinere Festplatte oder LUN verwendet wird, versucht das Installationsprogramm, einen Scratch-Bereich auf einer anderen lokalen Festplatte zuzuteilen. Wenn keine lokale Festplatte

gefunden wird, wird die Scratch-Partition `/scratch` auf der ESXi-Host-Ramdisk erstellt, die mit `/tmp/scratch` verknüpft ist. Sie können `/scratch` neu konfigurieren, um eine separate Festplatte oder LUN zu verwenden. Um eine bestmögliche Leistung zu erzielen und den Arbeitsspeicher zu optimieren, sollten Sie `/scratch` nicht auf der ESXi-Host-Ramdisk belassen.

Zum Neukonfigurieren von `/scratch` finden Sie weitere Informationen unter „Festlegen der Scratch-Partition vom vSphere Web Client aus", auf Seite 192.

Aufgrund der E/A-Empfindlichkeit von USB- und SD-Geräten erstellt das Installationsprogramm keine Scratch-Partition auf diesen Geräten. Beim Installieren oder Upgraden auf USB- bzw. SD-Geräten versucht das Installationsprogramm, einen Scratch-Bereich auf einer verfügbaren lokalen Festplatte oder einem lokalen Datenspeicher zuzuteilen. Wenn keine lokale Festplatte bzw. kein lokaler Datenspeicher gefunden wird, wird `/scratch` auf der Ramdisk abgelegt. Nach der Installation bzw. nach dem Upgrade sollten Sie `/scratch` neu konfigurieren, um einen dauerhaften Datenspeicher zu verwenden. Ein USB/SD-Gerät mit 1 GB reicht zwar für die Minimalinstallation aus, aber Sie sollten ein Gerät mit mindestens 4 GB verwenden. Der zusätzliche Speicher wird für eine erweiterte Coredump-Partition auf dem USB/SD-Gerät verwendet. Verwenden Sie ein qualitativ hochwertiges USB-Flash-Laufwerk mit mindestens 16 GB, sodass die zusätzlichen Flashzellen die Lebensdauer des Startmediums verlängern können, aber qualitativ hochwertige Laufwerke mit mindestens 4 GB reichen für die erweiterte Coredump-Partition aus. Weitere Informationen hierzu finden Sie im Knowledgebase-Artikel http://kb.vmware.com/kb/2004784.

Bei Auto Deploy-Installationen versucht das Installationsprogramm, einen Scratch-Bereich auf einer verfügbaren lokalen Festplatte oder einem lokalen Datenspeicher zuzuteilen. Wenn keine lokale Festplatte bzw. kein lokaler Datenspeicher gefunden wird, wird `/scratch` auf der Ramdisk abgelegt. Sie sollten `/scratch` neu konfigurieren, um nach der Installation einen dauerhaften Datenspeicher zu verwenden.

Bei Umgebungen, die von einem SAN starten oder Auto Deploy verwenden, ist es nicht erforderlich, eine separate LUN für jeden ESXi-Host zuzuteilen. Sie können die Scratch-Bereiche für viele ESXi-Hosts zusammen auf einer einzelnen LUN unterbringen. Die Anzahl der Hosts, die einer einzelnen LUN zugewiesen sind, sollten anhand der LUN-Größe und dem E/A-Verhalten der virtuellen Maschinen abgewogen werden.

Unterstützte Remotemanagement-Servermodelle und Firmware-Versionen

Sie können Remotemanagement-Anwendungen für die Installation bzw. das Upgrade von ESXi oder für die Remoteverwaltung von Hosts verwenden.

Tabelle 2-1. Unterstützte Remotemanagement-Servermodelle und Mindest-Firmware-Versionen

Remotemanagement-Servermodell	Firmware-Version	Java
Dell DRAC 7	1.30.30 (Build 43)	1.7.0_60-b19
Dell DRAC 6	1.54 (Build 15), 1.70 (Build 21)	1.6.0_24
Dell DRAC 5	1.0, 1.45, 1.51	1.6.0_20,1.6.0_203
Dell DRAC 4	1.75	1.6.0_23
HP ILO	1.81, 1.92	1.6.0_22, 1.6.0_23
HP ILO 2	1.8, 1.81	1.6.0_20, 1.6.0_23
HP ILO 3	1.28	1.7.0_60-b19
HP ILO 4	1.13	1.7.0_60-b19
IBM RSA 2	1.03, 1.2	1.6.0_22

Empfehlungen für verbesserte ESXi -Leistung

Installieren oder upgraden Sie ESXi zur Verbesserung der Leistung auf einem leistungsfähigen System mit mehr als dem erforderlichen Mindestwert an RAM und mit mehreren physischen Festplatten.

Weitere Informationen zu den ESXi-Systemanforderungen finden Sie unter „Hardwareanforderungen für ESXi“, auf Seite 21. Die technischen Unterlagen zur Leistung von vSphere 5 finden Sie unter http://www.vmware.com/resources/techresources/cat/91,203,96.

Tabelle 2-2. Empfehlungen zur Leistungssteigerung

Systemelement	Empfehlung
RAM	ESXi-Hosts benötigen mehr RAM-Speicher als übliche Server. Stellen Sie mindestens 8 GB RAM bereit, um alle Vorteile der ESXi-Funktionen optimal nutzen und virtuelle Maschinen in typischen Produktionsumgebungen ausführen zu können. Ein ESXi-Host muss über ausreichend RAM verfügen, um mehrere virtuelle Maschinen gleichzeitig auszuführen. Die folgenden Beispiele sollen Ihnen bei der Berechnung des RAM helfen, der von den virtuellen Maschinen benötigt wird, die auf dem ESXi-Host ausgeführt werden. Der Betrieb von vier virtuellen Maschinen mit Red Hat Enterprise Linux oder Windows XP erfordert mindestens 3 GB RAM für die Baseline-Leistung. Darin enthalten sind etwa 1024 MB für die virtuelle Maschinen, 256 MB Minimum für jedes Betriebssystem, wie von den Anbietern empfohlen. Die Ausführung dieser vier virtuelle Maschinen mit jeweils 512 MB RAM hat zur Folge, dass der ESXi-Host ungefähr 4 GB RAM haben muss, worin 2048 MB für die virtuelle Maschinen enthalten sind. Für diese Berechnungen wurde keine mögliche Einsparung von Arbeitsspeicher durch variable Overhead-Speicherkapazität für die einzelnen virtuelle Maschinen berücksichtigt. Siehe *vSphere-Ressourcenverwaltung*.
Dedizierte schnelle Ethernet-Adapter für virtuelle Maschinen	Verwenden Sie für Verwaltungsnetzwerke und Netzwerke virtueller Maschinen verschiedene physische Netzwerkkarten. Dedizierte Gigabit-Ethernet-Karten für virtuelle Maschinen, z.B. Intel PRO/1000-Adapter, verbessern den Durchsatz zu virtuelle Maschinen bei hohem Netzwerkdatenverkehr.
Festplattenspeicherort	Alle von den virtuelle Maschinen verwendeten Daten sollten sich auf physischen, den virtuelle Maschinen speziell zugeteilten Festplatten befinden. Sie können die Leistung steigern, wenn Sie Ihre virtuelle Maschinen nicht auf der Festplatte ablegen, die das ESXi-Boot-Image enthält. Verwenden Sie physische Festplatten, die groß genug sind, um Festplatten-Images aufzunehmen, die von allen virtuelle Maschinen verwendet werden.

Tabelle 2-2. Empfehlungen zur Leistungssteigerung (Fortsetzung)

Systemelement	Empfehlung
VMFS5-Partitionierung	Das ESXi-Installationsprogramm erstellt die anfänglichen VMFS-Volumes automatisch auf der ersten leeren gefundenen lokalen Festplatte. Verwenden Sie zum Hinzufügen von Festplatten oder zum Ändern der ursprünglichen Konfiguration den vSphere Web Client. Dadurch wird gewährleistet, dass die Startsektoren der Partitionen für 64 KB ausgerichtet sind, wodurch eine Verbesserung der Speicherleistung erzielt werden kann. **Hinweis** In reinen SAS-Umgebungen kann es vorkommen, dass das Installationsprogramm die Festplatten nicht formatiert. Bei manchen SAS-Festplatten ist es nicht möglich festzustellen, ob die Festplatten lokal oder remote sind. Nach der Installation können Sie den vSphere Web Client zum Einrichten von VMFS verwenden.
Prozessoren	Die ESXi-Leistung kann durch schnellere Prozessoren gesteigert werden. Für bestimmte Workloads verbessern größere Caches die Leistung von ESXi.
Hardwarekompatibilität	Verwenden Sie auf Ihrem Server Geräte, die von ESXi 6.0-Treibern unterstützt werden. Weitere Informationen finden Sie im *Hardware-Kompatibilitätshandbuch* unter http://www.vmware.com/resources/compatibility.

Ein- und ausgehende Firewall-Ports für ESXi-Hosts

Im vSphere Web Client können Sie für jeden Dienst die Firewall öffnen oder schließen oder den Datenverkehr aus bestimmten IP-Adressen durchlassen.

Die folgende Tabelle enthält die Firewalls für die üblicherweise installierten Dienste. Wenn Sie andere VIBs auf Ihrem Host installieren, stehen Ihnen möglicherweise weitere Dienste und Firewall-Ports zur Verfügung.

Tabelle 2-3. Eingehende Firewall-Verbindungen

Dienst	Port	Kommentar
CIM-Server	5988 (TCP)	Server für CIM (Common Information Model)
Sicherer CIM-Server	5989 (TCP)	Sicherer Server für CIM
CIM-SLP	427 (TCP, UDP)	Der CIM-Client verwendet das Service Location Protocol, Version 2 (SLPv2), zum Ermitteln von CIM-Servern.
DHCPv6	546 (TCP, UDP)	DHCP-Client für IPv6
DVSSync	8301, 8302 (UDP)	DVSSync-Ports werden zur Synchronisierung des Status von verteilten virtuellen Ports zwischen Hosts mit aktivierter VMware FT-Aufzeichnung und -Wiedergabe verwendet. Diese Ports dürfen nur für Hosts geöffnet sein, auf denen primäre oder Backup-VMs ausgeführt werden. Für Hosts ohne VMware FT dürfen diese Ports nicht geöffnet sein.
NFC	902 (TCP)	Network File Copy (NFC) umfasst einen FTP-Dienst für vSphere-Komponenten, bei dem der Dateityp beachtet wird. ESXi verwendet NFC standardmäßig für Vorgänge wie das Kopieren und Verschieben von Daten zwischen Datenspeichern.

Tabelle 2-3. Eingehende Firewall-Verbindungen (Fortsetzung)

Dienst	Port	Kommentar
Virtual SAN-Clusterbildungs-dienst	12345, 23451 (UDP)	Cluster-Überwachungs-, Mitgliedschafts- und Verzeichnisdienst für Virtual SAN. Verwendet UDP-basiertes IP-Multicast zur Bestimmung von Clustermitgliedern und Verteilung von Virtual SAN-Metadaten an alle Clustermitglieder. Wenn aktiviert, kann Virtual SAN nicht genutzt werden.
DHCP-Client	68 (UDP)	DHCP-Client für IPv4
DNS-Client	53 (UDP)	DNS-Client
Fault Tolerance	8200, 8100, 8300 (TCP, UDP)	Datenverkehr zwischen Hosts für vSphere Fault Tolerance (FT)
NSX Distributed Logical Router-Dienst	6999 (UDP)	NSX Virtual Distributed Logical Router-Dienst. Die Firewall für diesen Dienst wird geöffnet, wenn NSX-VIBs installiert werden und das VDR-Modul erstellt wird. Wenn keine VDR-Instanzen mit dem Host verbunden sind, muss der Port nicht geöffnet sein. In früheren Produktversionen wurde dieser Dienst als „NSX Distributed Logical Router“ bezeichnet.
Virtual SAN-Transport	2233 (TCP)	Zuverlässiger Datagramm-Transport für Virtual SAN. Verwendet TCP und dient der Virtual SAN-Speicher-E/A. Wenn aktiviert, kann Virtual SAN nicht genutzt werden.
SNMP-Server	161 (UDP)	Ermöglicht dem Host die Verbindung mit einem SNMP-Server.
SSH-Server	22 (TCP)	Erforderlich für SSH-Zugriff.
vMotion	8000 (TCP)	Erforderlich für die VM-Integration mit vMotion.
vSphere Web Client	902, 443 (TCP)	Client-Verbindungen
vsanvp	8080 (TCP)	VSAN-VASA-Anbieter-Provider. Wird vom Speicherverwaltungsdienst (Storage Management Service, SMS) im Umfang von vCenter für den Zugriff auf Daten zu Virtual SAN-Speicherprofilen, Funktionen und Compliance genutzt. Wenn deaktiviert, kann das Virtual SAN Storage Profile Based Management (SPBM) nicht genutzt werden.
vSphere Web Access	80 (TCP)	Begrüßungsseite mit Downloadlinks für verschiedene Schnittstellen

Tabelle 2-4. Ausgehende Firewall-Verbindungen

Dienst	Port	Kommentar
CIM-SLP	427 (TCP, UDP)	Der CIM-Client verwendet das Service Location Protocol, Version 2 (SLPv2), zum Ermitteln von CIM-Servern.
DHCPv6	547 (TCP, UDP)	DHCP-Client für IPv6
DVSSync	8301, 8302 (UDP)	DVSSync-Ports werden zur Synchronisierung des Status von verteilten virtuellen Ports zwischen Hosts mit aktivierter VMware FT-Aufzeichnung und -Wiedergabe verwendet. Diese Ports dürfen nur für Hosts geöffnet sein, auf denen primäre oder Backup-VMs ausgeführt werden. Für Hosts ohne VMware FT dürfen diese Ports nicht geöffnet sein.

Tabelle 2-4. Ausgehende Firewall-Verbindungen (Fortsetzung)

Dienst	Port	Kommentar
HBR	44046, 31031 (TCP)	Wird von vSphere Replication und VMware Site Recovery Manager für den laufenden Replizierungsdatenverkehr verwendet.
NFC	902 (TCP)	Network File Copy (NFC) umfasst einen FTP-Dienst für vSphere-Komponenten, bei dem der Dateityp beachtet wird. ESXi verwendet NFC standardmäßig für Vorgänge wie das Kopieren und Verschieben von Daten zwischen Datenspeichern.
WOL	9 (UDP)	Verwendet von „Wake on LAN“.
Virtual SAN-Clusterbildungsdienst	12345 23451 (UDP)	Cluster-Überwachungs-, Mitgliedschafts- und Verzeichnisdienst, verwendet von Virtual SAN
DHCP-Client	68 (UDP)	DHCP-Client
DNS-Client	53 (TCP, UDP)	DNS-Client
Fault Tolerance	80, 8200, 8100, 8300 (TCP, UDP)	Unterstützt VMware Fault Tolerance.
Software-iSCSI-Client	3260 (TCP)	Unterstützt Software-iSCSI.
NSX Distributed Logical Router-Dienst	6999 (UDP)	Die Firewall für diesen Dienst wird geöffnet, wenn NSX-VIBs installiert werden und das VDR-Modul erstellt wird. Wenn keine VDR-Instanzen mit dem Host verbunden sind, muss der Port nicht geöffnet sein.
rabbitmqproxy	5671 (TCP)	Ein auf dem ESXi-Host ausgeführter Proxy, der Hostanwendungen innerhalb von virtuellen Maschinen die Kommunikation mit den AMQP-Brokern in der vCenter-Netzwerkdomäne ermöglicht. Die virtuelle Maschine muss sich nicht im Netzwerk befinden, d. h., es ist keine Netzwerkkarte erforderlich. Der Proxy verbindet sich mit den Brokern in der vCenter-Netzwerkdomäne. Die IP-Adressen der ausgehenden Verbindungen müssen daher mindestens die aktuell oder zukünftig verwendeten Broker enthalten. Bei einer Erweiterung können zusätzliche Broker hinzugefügt werden.
Virtual SAN-Transport	2233 (TCP)	Wird für den RDT-Datenverkehr (Unicast-Peer-to-Peer-Kommunikation) zwischen Virtual SAN-Knoten verwendet.
vMotion	8000 (TCP)	Erforderlich für die VM-Integration mit vMotion.
VMware vCenter Agent	902 (UDP)	vCenter Server-Agent
vsanvp	8080 (TCP)	Wird für Virtual SAN-Anbieter-Provider-Datenverkehr verwendet.

Anforderungen für vCenter Server für Windows

Für die Installation von vCenter Server auf einer virtuellen Windows-Maschine oder einem physischen Server unter Windows muss Ihr System bestimmte Hardware- und Softwareanforderungen erfüllen.

- Synchronisieren Sie die Systemuhren der virtuellen Maschinen, auf denen Sie vCenter Server und den Platform Services Controller installieren möchten. Siehe „Synchronisieren der Systemuhren im vSphere-Netzwerk“, auf Seite 231.
- Der DNS-Name der virtuellen Maschine bzw. des physischen Servers muss mit dem tatsächlichen vollständigen Computernamen übereinstimmen.

- Stellen Sie sicher, dass der Hostname der virtuellen Maschine bzw. des physischen Servers, auf der/dem Sie vCenter Server installieren oder upgraden, mit den RFC 1123-Richtlinien übereinstimmt.
- Stellen Sie sicher, dass es sich bei dem System, auf dem vCenter Server installiert wird, nicht um einen Active Directory-Domänencontroller handelt.
- Wenn Ihr vCenter Server-Dienst in einem anderen Benutzerkonto als dem lokalen Systemkonto ausgeführt wird, stellen Sie sicher, dass das Benutzerkonto, in dem der vCenter Server-Dienst ausgeführt wird, über die folgenden Berechtigungen verfügt:
  - **Mitglied der Gruppe „Administratoren“**
  - **Anmelden als Dienst**
  - **Agieren als Teil des Betriebssystems (wenn der Benutzer ein Domänenbenutzer ist)**
- Wenn das System, das Sie für Ihre vCenter Server-Installation verwenden, einer Arbeitsgruppe und nicht einer Domäne angehört, sind in vCenter Server nicht alle Funktionen verfügbar. Wenn es einer Arbeitsgruppe zugeordnet wurde, kann das vCenter Server-System nicht alle Domänen und Systeme erkennen, die im Netzwerk verfügbar sind, wenn Funktionen verwendet werden. Ihre Hostmaschine muss mit einer Domäne verbunden sein, wenn Sie nach der Installation Active Directory-Identitätsquellen hinzufügen möchten.
- Vergewissern Sie sich, dass das Konto LOCAL SERVICE über Leseberechtigung sowohl für den Ordner, in dem vCenter Server installiert ist, als auch für die HKLM-Registrierung verfügt.
- Stellen Sie sicher, dass die Verbindung zwischen der virtuellen Maschine bzw. dem physischen Server und dem Domänencontroller funktioniert.

Prüfungen vor der Installation von vCenter Server für Windows

Bei der Installation oder dem Upgrade von vCenter Server und dem Platform Services Controller führt das Installationsprogramm eine Prüfung vor der Installation durch, um sicherzustellen, dass ausreichend Speicherplatz auf der virtuellen Maschine bzw. auf dem physischen Server verfügbar ist, wo vCenter Server installiert oder aktualisiert werden soll, und dass auf die ggf. vorhandene externe Datenbank zugegriffen werden kann.

Wenn Sie vCenter Server mit einem eingebetteten Platform Services Controller bzw. einem externen Platform Services Controller bereitstellen, wird vCenter Single Sign On als Teil des Platform Services Controller installiert. Zum Zeitpunkt der Installation bietet das Installationsprogramm die Möglichkeit, einer vorhandenen vCenter Single Sign On-Serverdomäne beizutreten. Wenn Sie die Informationen zum anderen vCenter Single Sign On-Dienst eingeben, überprüft das Installationsprogramm mithilfe des Administratorkontos den Hostnamen und das Kennwort, um sicherzustellen, dass die für den vCenter Single Sign On-Server eingegebenen Informationen authentifiziert werden können, bevor die Installation fortgesetzt wird.

Bei der Prüfung vor der Installation werden die folgenden Aspekte der Umgebung überprüft:

- Windows-Version
- Mindestanforderungen an den Prozessor
- Mindestanforderungen an den Arbeitsspeicher
- Mindestanforderungen an den Festplattenspeicher
- Berechtigungen für das ausgewählte Installations- und Datenverzeichnis
- Verfügbarkeit interner und externer Ports
- Version der externen Datenbank
- Konnektivität zur externen Datenbank
- Administratorrechte auf der Windows-Maschine

- Sämtliche eingegebene Anmeldedaten

Informationen zu den Mindestspeicheranforderungen erhalten Sie unter „Speicheranforderungen für vCenter Server für Windows“, auf Seite 29. Informationen zu den Mindesthardwareanforderungen erhalten Sie unter „Hardwareanforderungen für vCenter Server für Windows“, auf Seite 29.

Hardwareanforderungen für vCenter Server für Windows

Bei der Installation von vCenter Server auf einer virtuellen Maschine oder einem physischen Server unter Microsoft Windows muss Ihr System bestimmte Hardwareanforderungen erfüllen.

Sie können vCenter Server und den Platform Services Controller auf derselben virtuellen Maschine oder demselben physischen Server oder auf verschiedenen virtuellen Maschinen bzw. physischen Servern installieren. Wenn Sie vCenter Server mit einem eingebetteten Platform Services Controller installieren, installieren Sie vCenter Server und den Platform Services Controller auf derselben virtuellen Maschine bzw. demselben physischen Server. Wenn Sie vCenter Server mit einem externen Platform Services Controller installieren, installieren Sie zunächst den Platform Services Controller, der alle erforderlichen Dienste auf einer virtuellen Maschine bzw. einem physischen Server enthält, und anschließend installieren Sie vCenter Server und die vCenter Server-Komponenten auf einer anderen virtuellen Maschine bzw. einem anderen physischen Server.

HINWEIS Die Installation von vCenter Server auf einem Netzlaufwerk oder USB-Flash-Laufwerk wird nicht unterstützt.

Tabelle 2-5. Empfohlene Mindestanforderungen an die Hardware für die Installation von vCenter Server auf einer Windows-Maschine

	Platform Services Controller	Sehr kleine Umgebung (bis zu 10 Hosts, 100 virtuelle Maschinen)	Kleine Umgebung (bis zu 100 Hosts, 1000 virtuelle Maschinen)	Mittlere Umgebung (bis zu 400 Hosts, 4,000 virtuelle Maschinen)	Große Umgebung (bis zu 1,000 Hosts, 10,000 virtuelle Maschinen)
Anzahl der CPUs	2	2	4	8	16
Arbeitsspeicher	2 GB RAM	8 GB RAM	16 GB RAM	24 GB RAM	32 GB RAM

WICHTIG Für vCenter Server mit einem eingebetteten Platform Services Controller müssen Sie in Abhängigkeit von der Größe Ihrer Umgebung die Hardwareanforderungen für Platform Services Controller zu den Hardwareanforderungen für vCenter Server addieren.

Informationen zu Hardwareanforderungen für Ihre Datenbank finden Sie in der Datenbankdokumentation. Die Datenbankanforderungen gelten zusätzlich zu den Anforderungen von vCenter Server, sofern die Datenbank und vCenter Server auf derselben Maschine ausgeführt werden.

Speicheranforderungen für vCenter Server für Windows

Bei der Installation von vCenter Server muss Ihr System Mindestspeicheranforderungen erfüllen.

Die Speicheranforderungen pro Ordner sind abhängig vom Bereitstellungsmodell, das Sie installieren möchten. Während der Installation können Sie einen anderen Ordner als den Standardordner `C:\Programme\VMware` auswählen, um vCenter Server und den Platform Services Controller zu installieren. Sie können auch einen anderen Ordner als den Standardordner `C:\ProgramData\VMware\vCenterServer\` zum Speichern von Daten auswählen.

Tabelle 2-6. Mindestspeicheranforderungen für vCenter Server abhängig vom Bereitstellungsmodell

Standardordner	vCenter Server mit einem eingebetteten Platform Services Controller	vCenter Server mit einem externen Platform Services Controller	Externer Platform Services Controller
`Programme`	6 GB	6 GB	1 GB
`ProgramData`	8 GB	8 GB	2 GB
Systemordner (Zwischenspeicher für das MSI-Installationsprogramm)	3 GB	3 GB	1 GB

Softwareanforderungen für vCenter Server für Windows

Stellen Sie sicher, dass vCenter Server von Ihrem Betriebssystem unterstützt wird.

vCenter Server erfordert ein 64-Bit-Betriebssystem sowie den 64-Bit-System-DSN zum Herstellen einer Verbindung mit der externen Datenbank.vCenter Server

Windows Server 2008 SP2 ist die älteste Windows Server-Version, die von vCenter Server unterstützt wird. Auf dem Windows-Server müssen die neuesten Updates und Patches installiert sein. Eine vollständige Aufstellung der unterstützten Betriebssysteme finden Sie unter http://kb.vmware.com/kb/2091273.

Datenbankanforderungen für vCenter Server für Windows

vCenter Server benötigt eine Datenbank zum Speichern und Organisieren von Serverdaten.

Für jede vCenter Server-Instanz ist eine eigene Datenbank erforderlich. Für Umgebungen mit bis zu 20 Hosts und bis zu 200 virtuellen Maschinen können Sie die mitgelieferte PostgreSQL-Datenbank verwenden, die das vCenter Server-Installationsprogramm während der Installation von vCenter Server für Sie installieren und einrichten kann. Eine größere Installation erfordert eine für die Größe der Umgebung unterstützte externe Datenbank.

Beim Installieren oder Upgraden von vCenter Server müssen Sie die eingebettete Datenbank installieren oder einen Verweis auf eine vorhandene unterstützte Datenbank für das vCenter Server-System angeben. vCenter Server unterstützt Oracle- und Microsoft SQL Server-Datenbanken. Informationen zu unterstützten Datenbankserverversionen finden Sie in der VMware-Produkt-Interoperabilitätstabelle unter http://www.vmware.com/resources/compatibility/sim/interop_matrix.php.

Anforderungen für die vCenter Server Appliance

Die vCenter Server Appliance kann auf einem ESXi-Host der Version 5.0 oder höher oder auf einer vCenter Server-Instanz der Version 5.0 oder höher bereitgestellt werden. Ihr System muss auch bestimmte Software- und Hardwareanforderungen erfüllen.

Wenn Sie vollqualifizierte Domänennamen verwenden, stellen Sie sicher, dass die Maschine, die Sie zum Bereitstellen der vCenter Server Appliance verwenden, und der ESXi-Host sich auf demselben DNS-Server befinden.

Bevor Sie die vCenter Server Appliance bereitstellen, sollten Sie die Systemuhren aller virtuellen Maschinen im vSphere-Netzwerk synchronisieren. Nicht synchronisierte Systemuhren können Authentifizierungsprobleme und einen Fehlschlag der Installation verursachen bzw. das Starten der vCenter Server-Dienste verhindern. Siehe „Synchronisieren der Systemuhren im vSphere-Netzwerk“, auf Seite 231.

Hardwareanforderungen für die vCenter Server Appliance

Bei der Bereitstellung der vCenter Server Appliance können Sie eine für die Größe Ihrer vSphere-Umgebung geeignete Appliance bereitstellen. Die gewählte Option bestimmt die Anzahl der CPUs und den Umfang des Arbeitsspeichers für die Appliance.

Die Hardwareanforderungen wie beispielsweise die Anzahl der CPUs und der Arbeitsspeicher hängen von der Größe Ihrer vSphere-Bestandsliste ab.

Tabelle 2-7. Hardwareanforderungen für die VMware vCenter Server Appliance

Ressourcen	Platform Services Controller	Sehr kleine Umgebung (bis zu 10 Hosts, 100 virtuelle Maschinen)	Kleine Umgebung (bis zu 100 Hosts, 1,000 virtuelle Maschinen)	Mittlere Umgebung (bis zu 400 Hosts, 4,000 virtuelle Maschinen)	Große Umgebung (bis zu 1,000 Hosts, 10,000 virtuelle Maschinen)
Anzahl der CPUs	2	2	4	8	16
Arbeitsspeicher	2 GB RAM	8 GB RAM	16 GB RAM	24 GB RAM	32 GB RAM

WICHTIG Für vCenter Server Appliance mit einem eingebetteten Platform Services Controller müssen Sie in Abhängigkeit von der Größe Ihrer Umgebung die Hardwareanforderungen für Platform Services Controller zu den Hardwareanforderungen für vCenter Server Appliance addieren.

Speicheranforderungen für die vCenter Server Appliance

Bei der Bereitstellung der vCenter Server Appliance muss der Host, auf dem Sie die Appliance bereitstellen, Mindestspeicheranforderungen erfüllen. Der erforderliche Speicher ist nicht nur von der Größe der vSphere-Umgebung abhängig, sondern auch vom Festplattenbereitstellungsmodus.

Die Speicheranforderungen hängen vom gewählten Bereitstellungsmodell ab.

Tabelle 2-8. Mindestspeicheranforderungen für vCenter Server abhängig vom Bereitstellungsmodell

	vCenter Server Appliance mit einem eingebetteten Platform Services Controller	vCenter Server Appliance mit einem externen Platform Services Controller	Externe Platform Services Controller-Appliance
Sehr kleine Umgebung (bis zu 10 Hosts, 100 virtuelle Maschinen)	120 GB	86 GB	30 GB
Kleine Umgebung (bis zu 100 Hosts, 1,000 virtuelle Maschinen)	150 GB	108 GB	30 GB
Mittlere Umgebung (bis zu 400 Hosts, 4000 virtuelle Maschinen)	300 GB	220 GB	30 GB
Große Umgebung (bis zu 1,000 Hosts, 10,000 virtuelle Maschinen)	450 GB	280 GB	30 GB

Im Lieferumfang der vCenter Server Appliance enthaltene Software

Die vCenter Server Appliance ist eine vorkonfigurierte Linux-basierte virtuelle Maschine, die für die Ausführung von vCenter Server und zugehörigen Diensten optimiert ist.

Das vCenter Server Appliance-Paket enthält die folgende Software:

- SUSE Linux Enterprise Server 11 Update 3 für VMware, 64-Bit-Edition
- PostgreSQL
- vCenter Server 6.0 und vCenter Server 6.0-Komponenten.

Softwareanforderungen für vCenter Server Appliance

Die VMware vCenter Server Appliance kann auf ESXi-Hosts der Version 5.0 oder höher oder auf vCenter Server-Instanzen der Version 5.0 oder höher bereitgestellt werden.

Die Bereitstellung der vCenter Server Appliance kann nur über das Client-Integrations-Plug-In erfolgen. Dabei handelt es sich um ein HTML-Installationsprogramm für Windows, mit dem Sie eine Verbindung mit dem Zielserver herstellen und die vCenter Server Appliance auf dem Server bereitstellen können. Sie können eine direkte Verbindung mit einem ESXi 5.0.x-, ESXi 5.1.x-, ESXi 5.5.x- oder ESXi 6.0.x-Host herstellen, auf dem die Appliance bereitgestellt werden soll. Darüber hinaus können Sie eine Verbindung mit einer vCenter Server 5.0.x-, vCenter Server 5.1.x.-, vCenter Server 5.5.x- oder vCenter Server 6.0.x-Instanz herstellen, um die Appliance auf einem ESXi-Host oder DRS-Cluster bereitzustellen, der sich in der vCenter Server-Bestandsliste befindet.

WICHTIG Sie können die vCenter Server Appliance nicht mit dem vSphere Client oder vSphere Web Client bereitstellen. Bei der Bereitstellung der vCenter Server Appliance müssen Sie verschiedene Informationen eingeben, wie z. B. die Kennwörter des Betriebssystems und von vCenter Single Sign-On. Wenn Sie versuchen, die Appliance mit dem vSphere Client oder vSphere Web Client bereitzustellen, werden Sie nicht zur Eingabe dieser Informationen aufgefordert und die Bereitstellung schlägt fehl.

Datenbankanforderungen für die vCenter Server Appliance

Die vCenter Server Appliance benötigt eine Datenbank zum Speichern und Organisieren von Serverdaten.

Für jede vCenter Server Appliance-Instanz ist eine eigene Datenbank erforderlich. Sie können die PostgreSQL-Datenbank verwenden, die im Lieferumfang der vCenter Server Appliance enthalten ist und bis zu 1000 Hosts und bis zu 10.000 virtuelle Maschinen unterstützt.

Für externe Datenbanken unterstützt die vCenter Server Appliance nur Oracle-Datenbanken. Diese Oracle-Datenbanken weisen die gleichen Versionen, die in der VMware-Produkt-Interoperabilitätsmatrix für die Version der vCenter Server-Instanz, die Sie installieren, angezeigt werden. Siehe die VMware-Produkt-Interoperabilitätsmatrix unter http://www.vmware.com/resources/compatibility/sim/interop_matrix.php.

Wenn Sie mit einer externen Datenbank arbeiten möchten, müssen Sie ein 64-Bit-DSN erstellen, damit vCenter Server eine Verbindung mit der Oracle-Datenbank herstellen kann.

Erforderliche Ports für vCenter Server

Das vCenter Server-System unter Windows und in der Appliance muss in der Lage sein, Daten an jeden verwalteten Host zu senden und Daten vom vSphere Web Client und von den Platform Services Controller-Diensten zu empfangen. Die Quell- und Zielhosts müssen Daten untereinander austauschen können, um Migrations- und Bereitstellungsaktivitäten zwischen verwalteten Hosts zu ermöglichen.

Wenn ein Port verwendet wird oder gesperrt ist, zeigt das Installationsprogramm für vCenter Server eine Fehlermeldung an. Sie müssen eine andere Portnummer verwenden, um mit der Installation fortfahren zu können. Es gibt interne Ports, die nur für den Datenaustausch zwischen Prozessen verwendet werden.

Für die Kommunikation verwendet VMware festgelegte Ports. Zudem überwachen die verwalteten Hosts die festgelegten Ports auf Daten von vCenter Server. Falls zwischen diesen Elementen eine Firewall vorhanden ist, öffnet das Installationsprogramm die Ports während der Installation bzw. des Upgrades. Für benutzerdefinierte Firewalls müssen die erforderlichen Ports manuell geöffnet werden. Wenn sich eine Firewall zwischen zwei von verwalteten Hosts befindet und Sie Quell- oder Zielaktivitäten wie z. B. eine Migration oder einen Klonvorgang ausführen möchten, muss der verwaltete Host Daten empfangen können.

Hinweis Unter Microsoft Windows Server 2008 oder höher ist die Firewall standardmäßig aktiviert.

Tabelle 2-9. Erforderliche Ports zur Kommunikation zwischen Komponenten

Port	Beschreibung	Kann während der Installation geändert werden
22	System-Port für SSHD. Dieser Port wird nur von der vCenter Server Appliance verwendet.	Nein
80	vCenter Server benötigt Port 80 für direkte HTTP-Verbindungen. Port 80 leitet Anforderungen an HTTPS-Port 443 weiter. Diese Umleitung ist nützlich, falls Sie versehentlich http://server anstelle von https://server verwenden. WS-Management (Port 443 muss ebenfalls offen sein). Wenn Sie eine Microsoft SQL-Datenbank verwenden, die auf derselben virtuellen Maschine oder demselben physischen Server wie vCenter Server gespeichert ist, wird Port 80 vom SQL Reporting-Dienst verwendet. Bei der Installation bzw. dem Upgrade von vCenter Server werden Sie vom Installationsprogramm aufgefordert, den HTTP-Port für vCenter Server zu ändern. Ändern Sie den HTTP-Port für vCenter Server in einen benutzerdefinierten Wert, um eine erfolgreiche Installation bzw. ein erfolgreiches Upgrade sicherzustellen.	Ja
88	KD-Center-Port von VMware.	Nein
389	Sowohl auf der lokalen als auch auf allen Remote-Instanzen von vCenter Server muss dieser Port geöffnet sein. Dies ist die LDAP-Portnummer für die Verzeichnisdienste der vCenter Server-Gruppe. Wenn auf diesem Port ein anderer Dienst ausgeführt wird, ist es in manchen Fällen empfehlenswert, diesen zu löschen oder einen anderen Port zuzuweisen. Sie können den LDAP-Dienst auf jedem Port zwischen 1025 und 65535 ausführen. Sofern diese Instanz als das Microsoft Windows Active Directory dient, ändern Sie die Portnummer von 389 in die Nummer eines verfügbaren Ports zwischen 1025 und 65535.	Nein
443	Der Standardport, den das vCenter Server-System zum Überwachen von Verbindungen vom vSphere Web Client verwendet. Öffnen Sie Port 443 in der Firewall, um dem vCenter Server-System den Empfang von Daten vom vSphere Web Client zu ermöglichen. Das vCenter Server-System verwendet Port 443 auch zur Überwachung der Datenübertragung zwischen SDK-Clients. Dieser Port wird auch für die folgenden Dienste verwendet: ■ WS-Management (Port 80 muss offen sein) ■ Verbindungen von Netzwerkverwaltungs-Clients von Drittanbietern mit vCenter Server ■ Zugriff von Netzwerkverwaltungs-Client von Drittanbietern auf Hosts	Ja
514	Port für vSphere Syslog Collector für vCenter Server unter Windows und Port für vSphere Syslog-Dienst für vCenter Server Appliance	Ja

Tabelle 2-9. Erforderliche Ports zur Kommunikation zwischen Komponenten (Fortsetzung)

Port	Beschreibung	Kann während der Installation geändert werden
636	Im Falle des erweiterten verknüpften Modus von vCenter Server ist dies der SSL-Port der lokalen Instanz. Wenn auf diesem Port ein anderer Dienst ausgeführt wird, ist es in manchen Fällen empfehlenswert, diesen zu löschen oder einen anderen Port zuzuweisen. Sie können den SSL-Dienst auf jedem Port zwischen 1025 und 65535 ausführen.	Nein
902	Der Standardport, den das vCenter Server-System zum Senden von Daten an verwaltete Hosts verwendet. Verwaltete Hosts senden außerdem regelmäßig Taktsignale über den UDP-Port 902 an das vCenter Server-System. Dieser Port darf nicht durch Firewalls zwischen dem Server und den Hosts bzw. zwischen Hosts blockiert werden. Port 902 darf nicht zwischen dem vSphere-Client und den Hosts blockiert werden. Der vSphere-Client verwendet diesen Port zum Anzeigen der Konsolen von virtuellen Maschinen.	Ja
1514	TLS-Port für vSphere Syslog Collector für vCenter Server unter Windows und TLS-Port für vSphere Syslog-Dienst für vCenter Server Appliance	Ja
2012	RPC des Schnittstellen-Steuerelements für vCenter Single Sign On	Nein
2014	RPC-Port für alle APIs von VMCA (VMware-Zertifizierungsstelle)	Ja
2020	Verwaltung des Authentifizierungsframeworks	Ja
6500	ESXi Dump Collector-Port	Ja
6501	Auto Deploy-Dienst	Ja
6502	Auto Deploy-Verwaltung	Ja
7444	Secure Token Service	Nein
9443	vSphere Web Client HTTPS	Nein
11711	LDAP von vCenter Single Sign On	Nein
11712	LDAPS von vCenter Single Sign On	Nein

Wenn das vCenter Server-System einen anderen Port zum Empfangen von vSphere Web Client-Daten verwenden soll, lesen Sie die Dokumentation *vCenter Server und Hostverwaltung*.

Weitere Informationen zur Firewall-Konfiguration finden Sie in der Dokumentation *vSphere-Sicherheit*.

DNS-Anforderungen für vSphere

Sie installieren oder upgraden vCenter Server, wie alle anderen Netzwerkserver auch, auf einem Computer mit einer festen IP-Adresse und einem bekannten DNS-Namen, damit Clients einen verlässlichen Zugriff auf den Dienst haben.

Weisen Sie dem Windows-Server, der das vCenter Server-System hosten soll, eine statische IP-Adresse und einen Hostnamen zu. Diese IP-Adresse muss eine gültige (interne) Registrierung für das DNS (Domain Name System) haben. Wenn Sie vCenter Server und den Platform Services Controller installieren, müssen Sie den vollqualifizierten Domänennamen (FQDN) oder die statische IP-Adresse der Hostmaschine, auf der Sie die Installation bzw. das Upgrade durchführen, angeben. Es wird empfohlen, den FQDN zu verwenden.

Bei der Bereitstellung der vCenter Server Appliance können Sie der Appliance eine statische IP-Adresse zuweisen. Dadurch stellen Sie sicher, dass bei einem Neustart des Systems die IP-Adresse der vCenter Server Appliance unverändert bleibt.

Stellen Sie sicher, dass das DNS-Reverse-Lookup einen FQDN zurückgibt, wenn dieser mit der IP-Adresse der Hostmaschine abgefragt wird, auf der vCenter Server installiert ist. Bei der Installation bzw. beim Upgrade von vCenter Server schlägt die Installation bzw. das Upgrade der Webserverkomponente, die den vSphere Web Client unterstützt, fehl, wenn das Installationsprogramm den vollqualifizierten Domänennamen der Hostmaschine von vCenter Server nicht über die IP-Adresse abrufen kann. Das Reverse-Lookup wird unter Verwendung von PTR Records implementiert.

Wenn Sie DHCP anstelle einer statischen IP-Adresse für vCenter Server verwenden, stellen Sie sicher, dass der vCenter Server-Computername im DNS (Domain Name Service) aktualisiert ist. Ist der Ping-Test mit dem Computernamen erfolgreich, wurde der Name im DNS aktualisiert.

Stellen Sie sicher, dass die Verwaltungsschnittstelle des ESXi-Hosts von der vCenter Server-Instanz und allen vSphere Web Client-Instanzen aus eine gültige DNS-Auflösung hat. Stellen Sie sicher, dass der vCenter Server von allen ESXi-Hosts und allen vSphere Web Client-Instanzen aus eine gültige DNS-Auflösung hat.

Überprüfen, ob der FQDN ausgelöst werden kann

Sie installieren oder upgraden vCenter Server, wie alle anderen Netzwerkserver auch, auf einer virtuellen Maschine oder einem physischen Server mit einer festen IP-Adresse und einem bekannten DNS-Namen, damit Clients einen verlässlichen Zugriff auf den Dienst haben.

Wenn Sie für die virtuelle Maschine oder den physischen Server, auf der/dem Sie vCenter Server installieren oder aktualisieren, einen vollständig qualifizierten Domänennamen (FQDN) verwenden möchten, müssen Sie prüfen, ob der FQDN auflösbar ist.

Vorgehensweise

◆ Führen Sie bei der Windows-Befehlseingabeaufforderung den Befehl `nslookup` aus.

```
nslookup –nosearch –nodefname your_vCenter_Server_FQDN
```

Wenn der FQDN aufgelöst werden kann, gibt der Befehl `nslookup` die IP-Adresse und den Namen der virtuellen Maschine oder des physischen Servers des vCenter Server zurück.

Softwareanforderungen für den vSphere Web Client

Stellen Sie sicher, dass Ihr Browser vSphere Web Client unterstützt.

Für vSphere Web Client 6.0 ist Adobe Flash Player 16 oder höher erforderlich. Die neueste Adobe Flash Player-Version für Linux-Systeme ist 11.2. Deshalb kann der vSphere Web Client nicht auf Linux-Plattformen ausgeführt werden.

VMware unterstützt die folgenden getesteten Gastbetriebssysteme und Browserversionen für vSphere Web Client: Verwenden Sie Google Chrome für bestmögliche Leistung.

Tabelle 2-10. Unterstützte Gastbetriebssysteme und Browsermindestversionen für den vSphere Web Client

Betriebssystem	Browser
Windows	Microsoft Internet Explorer 10.0.19 oder höher. Mozilla Firefox 34 und höher. Google Chrome 39 und höher.
Mac OS	Mozilla Firefox 34 und höher. Google Chrome 39 und höher.

Softwareanforderungen für das Client-Integrations-Plug-In

Wenn Sie das Client-Integrations-Plug-In unabhängig vom vSphere Web Client installieren möchten, sodass Sie sich mit einem ESXi-Host verbinden und die vCenter Server Appliance bereitstellen oder aktualisieren können, stellen Sie sicher, dass Ihr Browser das Client-Integrations-Plug-In unterstützt.

Bevor Sie das Client-Integrations-Plug-In verwenden können, prüfen Sie, ob Sie einen der unterstützten Webbrowser haben.

Tabelle 2-11. Unterstützte Webbrowser

Browser	Unterstützte Versionen
Microsoft Internet Explorer	Version 10 oder 11
Mozilla Firefox	Version 30 oder höher
Google Chrome	Version 35 oder höher

vSphere Client-Anforderungen

Sie können den vSphere Client zum Verwalten eines einzelnen ESXi-Hosts installieren. Das Windows-System, auf dem Sie vSphere Client installieren, muss bestimmte Hardware- und Softwareanforderungen erfüllen.

vSphere-Client-Hardwareanforderungen

Stellen Sie sicher, dass die vSphere-Client-Hardware die Mindestanforderungen erfüllt.

Mindestanforderungen an die Hardware und Hardwareempfehlungen für den vSphere-Client

Tabelle 2-12. Mindestanforderungen an die Hardware und Hardwareempfehlungen für den vSphere-Client

vSphere-Client-Hardware	Anforderungen und Empfehlungen
CPU	1 CPU
Prozessor	500 MHz oder schnellerer Intel- oder AMD-Prozessor (1 GHz empfohlen)
Arbeitsspeicher	500 MB (1 GB empfohlen)

Tabelle 2-12. Mindestanforderungen an die Hardware und Hardwareempfehlungen für den vSphere-Client (Fortsetzung)

vSphere-Client-Hardware	Anforderungen und Empfehlungen
Festplattenspeicher	1,5 GB freier Festplattenspeicher für eine Komplettinstallation mit den folgenden Komponenten: ■ Microsoft .NET 2.0 SP2 ■ Microsoft .NET 3.0 SP2 ■ Microsoft .NET 3.5 SP1 ■ Microsoft Visual J# Entfernen Sie alle vorherigen Versionen von Microsoft Visual J# von dem System, auf dem Sie den vSphere-Client installieren möchten. ■ vSphere Client Wenn keine der Komponenten bereits installiert sind, werden 400 MB an freien Speicherplatz auf dem Laufwerk benötigt, auf dem sich das `%temp%`-Verzeichnis befindet. Wenn alle Komponenten bereits installiert sind, werden 300 MB an freiem Speicherplatz auf dem Laufwerk benötigt, auf dem sich das Verzeichnis`%temp%` befindet, und 450 MB sind für vSphere-Client erforderlich.
Netzwerk	Gigabit-Verbindung empfohlen

Softwareanforderungen des vSphere Clients

Stellen Sie sicher, dass vSphere Client von Ihrem Betriebssystem unterstützt wird.

Eine vollständige aktuelle Liste der unterstützten Betriebssysteme für den vSphere Client finden Sie unter Unterstützte Hostbetriebssysteme für die vSphere Client (Windows)-Installation.

Der vSphere-Client benötigt das Microsoft .NET 3.5 SP1 Framework. Falls dieses nicht auf Ihrem System installiert ist, wird es vom vSphere-Client-Installationsprogramm installiert. Für die .NET 3.5 SP1-Installation wird möglicherweise eine Internetverbindung zum Herunterladen zusätzlicher Dateien benötigt.

TCP- und UDP-Ports für den vSphere Client

Der Zugriff auf ESXi-Hosts und andere Netzwerkkomponenten erfolgt über vorab festgelegte TCP- und UDP-Ports. Wenn Netzwerkkomponenten, die außerhalb einer Firewall liegen, verwaltet werden müssen, muss ggf. die Firewall neu konfiguriert werden, damit auf die entsprechenden Ports zugegriffen werden kann.

Die Tabelle enthält eine Auflistung von TCP- und UDP-Ports mit dem jeweiligen Zweck und Typ. Bei der Installation standardmäßig geöffnete Ports werden angegeben (Standard).

Tabelle 2-13. TCP- und UDP-Ports

Port	Zweck	Art des Datenverkehrs
443 (Standard)	HTTPS-Zugriff vSphere-Clientzugriff auf vCenter Server vSphere-Client-Zugriff auf ESXi-Hosts vCenter Server-Zugriff auf vSphere Update Manager	Eingehendes TCP
902 (Standard)	vSphere-Client-Zugriff auf die Konsolen virtueller Maschinen	Eingehendes und ausgehendes TCP, ausgehendes UDP
903	Datenverkehr der Remotekonsole, der durch Zugriffe der Benutzer auf virtuelle Maschinen auf einem bestimmten Host entsteht. vSphere-Client-Zugriff auf die Konsolen virtueller Maschinen MKS-Transaktionen (xinetd/vmware-authd-mks)	Eingehendes TCP

Erforderlicher freier Speicherplatz für die Systemprotokollierung

Wenn Sie Auto Deploy für die Installation Ihres ESXi 6.0-Hosts verwendet haben oder wenn Sie ein Protokollverzeichnis nicht im Standardverzeichnis, sondern in einem Scratch-Verzeichnis auf dem VMFS-Volume eingerichtet haben, müssen Sie möglicherweise die aktuellen Einstellungen für die Protokollgröße und die Rotation ändern, um sicherzustellen, dass ausreichend Speicherplatz für die Systemprotokollierung verfügbar ist.

Alle vSphere-Komponenten verwenden diese Infrastruktur. Die Standardwerte für die Protokollkapazität in dieser Infrastruktur variieren je nach verfügbarem Speicherplatz und je nach Konfiguration der Systemprotokollierung. Hosts, die mit Auto Deploy bereitgestellt werden, speichern Protokolle auf einer RAM-Festplatte. Der verfügbare Speicherplatz für Protokolle ist daher gering.

Wenn Ihr Host mit Auto Deploy bereitgestellt wurde, stehen Ihnen für die Konfiguration des Protokollspeichers folgende Möglichkeiten zur Verfügung:

- Leiten Sie die Protokolle über das Netzwerk zu einem Remote-Controller um.
- Leiten Sie die Protokolle zu einem NAS- oder NFS-Speicher um.

Wenn Sie Protokolle an einen nicht standardmäßigen Speicher umleiten, zum Beispiel an einen NAS- oder NFS-Speicher, können Sie die Größe und Rotation der auf der Festplatte installierten Hosts ebenfalls neu konfigurieren.

Sie müssen den Protokollspeicher für ESXi-Hosts nicht neu konfigurieren, die die Standardkonfiguration verwenden, bei der Protokolle in einem Scratch-Verzeichnis auf dem VMFS-Volume gespeichert werden. Für diese Hosts konfiguriert ESXi 6.0 die Protokolle in optimaler Abstimmung mit Ihrer Installation und bietet ausreichend Speicherplatz für Protokollnachrichten.

Tabelle 2-14. Empfohlene Mindestgröße und Rotationskonfiguration für hostd-, vpxa- und fdm-Protokolle

Protokoll	Maximale Protokolldateigröße	Anzahl der beizubehaltenden Rotationen	Mindestens erforderlicher Festplattenspeicher
Verwaltungs-Agent (hostd)	10 MB	10	100 MB
VirtualCenter Agent (vpxa)	5 MB	10	50 MB
vSphere HA-Agent (Fault Domain Manager, fdm)	5 MB	10	50 MB

Informationen zum Einrichten eines Remoteprotokollservers finden Sie unter „Konfiguration von Syslog auf ESXi-Hosts“, auf Seite 195.

Vor der Installation von ESXi 3

Vor der ESXi-Installation sollten Sie mit dem Installationsverfahren und den Installationsoptionen vertraut sein.

Dieses Kapitel behandelt die folgenden Themen:

Optionen für die Installation von ESXi

Es gibt mehrere Möglichkeiten zum Installieren von ESXi. Bevor Sie mit der Installation beginnen, machen Sie sich mit den Optionen gründlich vertraut, um die beste vSphere-Bereitstellung sicherzustellen.

ESXi-Installationen ermöglichen eine gewisse Bandbreite bei der Größe von Bereitstellungen.

Je nach dem gewählten Installationsverfahren sind mehrere Optionen für das Zugreifen auf das Installationsmedium und für das Starten des Installationsprogramms verfügbar.

Interaktive ESXi-Installation

Die interaktive Installation wird für kleine Bereitstellungen von weniger als fünf Hosts empfohlen.

Sie starten das Installationsprogramm von einer CD bzw. DVD, von einem startfähigen USB-Gerät oder per PXE-Startvorgang von einem Speicherort im Netzwerk. Sie befolgen die Aufforderungen des Installationsassistenten, um ESXi auf einer Festplatte zu installieren. Weitere Informationen hierzu finden Sie unter „Interaktives Installieren von ESXi", auf Seite 57.

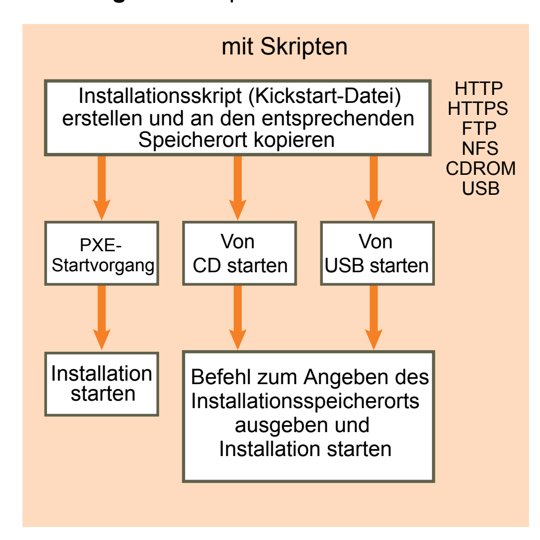
ESXi-Installation im Skriptmodus

Das Ausführen eines Skripts ist eine effiziente Möglichkeit, um mehrere ESXi-Hosts in einer unbeaufsichtigten Installation bereitzustellen.

Das Installationsskript enthält die Einstellungen für die Hostkonfiguration. Sie können das Skript zur Konfiguration mehrerer Hosts mit denselben Einstellungen verwenden. Weitere Informationen hierzu finden Sie unter „Installieren oder Upgraden von Hosts mithilfe eines Skripts", auf Seite 60.

Das Installationsskript muss sich an einem Speicherort befinden, auf den der Host über HTTP, HTTPS, FTP, NFS, CD-ROM oder USB zugreifen kann. Sie können das ESXi-Installationsprogramm per PXE-Startvorgang starten oder es von einem CD-/DVD- oder USB-Laufwerk starten.

Abbildung 3-1. Skriptinstallation



Auto Deploy ESXi-Installation

vSphere 5.x und vSphere 6.0 bieten mehrere Möglichkeiten zum Installieren von ESXi mit Auto Deploy.

Diese Themen beschreiben die Auto Deploy-Optionen für die Installation von ESXi.

Bereitstellen von ESXi -Hosts unter Verwendung von vSphere Auto Deploy

Mit der ESXi-Funktion von vSphere Auto Deploy können Sie eine große Anzahl an ESXi-Hosts mit vCenter Server effizient bereitstellen und neu bereitstellen.

Wenn Sie Hosts mithilfe der Auto Deploy-Funktion bereitstellen, lädt vCenter Server das ESXi-Image direkt in den Hostarbeitsspeicher. Auto Deploy speichert den ESXi-Status nicht auf der Host-Festplatte.

vCenter Server stellt ESXi-Updates und Patches zum Herunterladen in Form eines Image-Profils zur Verfügung. Optional wird die Hostkonfiguration in Form eines Hostprofils zur Verfügung gestellt. Mit vSphere Web Client können Sie Hostprofile erstellen. Sie können benutzerdefinierte Image-Profile mit der ESXi Image Builder CLI erstellen. Siehe „Verwenden von vSphere ESXi Image Builder“, auf Seite 149 und *vSphere-Hostprofile*.

Bei der ersten Bereitstellung eines Hosts mit Auto Deploy wird der Host-PXE-Startvorgang eingeleitet und eine Verbindung mit dem Auto Deploy-Server hergestellt, der ein Streaming des Image-Profils und etwaiger Hostprofile auf den Host durchführt. Der Host startet mit dem Image-Profil, und Auto Deploy weist den Host dem entsprechenden vCenter Server-System zu.

Wenn Sie den Host neu starten, fährt der Auto Deploy-Server mit dem Bereitstellen des Hosts mit dem entsprechenden Image- und Hostprofil fort. Um den Host mit einem anderen Image-Profil auszustatten, müssen Sie die Regel ändern, die das Image-Profil spezifiziert, und einen Vorgang zum Testen und Reparieren von Übereinstimmungen durchführen. Ändern Sie die Regel und führen Sie Test und Reparatur durch, um die Änderungen an alle in der Regel angegebenen Hosts weiterzugeben. Die Fähigkeit zum Weitergeben von Änderungen an mehrere Hosts macht aus Auto Deploy ein effizientes Werkzeug zum Bereitstellen und erneuten Bereitstellen einer großen Anzahl Hosts sowie zum Durchsetzen der Übereinstimmung mit einem Master-ESXi-Image.

Weitere Informationen hierzu finden Sie unter „Grundlegendes zu vSphere Auto Deploy“, auf Seite 76.

Verwenden von vSphere Auto Deploy für statusorientierte Installationen

In einigen Situationen ist es nützlich, Hosts mit Auto Deploy bereitzustellen und alle anschließenden Startvorgänge von der Festplatte aus durchzuführen.

Sie können vSphere Auto Deploy verwenden, um einen ESXi-Host bereitzustellen und ein Hostprofil einzurichten, das dafür sorgt, dass der Host das ESXi-Image und die Konfiguration auf einer lokalen Festplatte, einer Remotefestplatte oder einem USB-Laufwerk speichert. Danach wird der ESXi-Host mithilfe dieses lokalen Images gestartet. Auto Deploy stellt den Host nicht mehr bereit. Dieser Prozess ähnelt dem Ausführen einer Skriptinstallation. Bei einer Skriptinstallation wird ein Host bereitgestellt und der Host wird dann von der Festplatte gestartet. In diesem Fall stellt Auto Deploy einen Host bereit und der Host wird dann von der Festplatte gestartet.

Weitere Informationen hierzu finden Sie unter „Verwenden von Auto Deploy für statusfreies Caching und statusorientierte Installationen“, auf Seite 101.

vSphere Auto Deploy und statusfreies Caching

Sie können vSphere Auto Deploy verwenden, um einen ESXi-Host bereitzustellen und ein Hostprofil einzurichten, das dafür sorgt, dass der Host das ESXi-Image und die Konfiguration auf einer lokalen Festplatte, einer Remotefestplatte oder einem USB-Laufwerk speichert.

Danach setzt der Auto Deploy-Server die Bereitstellung für diesen Host fort. Wenn der Auto Deploy-Server nicht verfügbar ist, verwendet der Host das Image auf der Festplatte.

Weitere Informationen hierzu finden Sie unter „Verwenden von Auto Deploy für statusfreies Caching und statusorientierte Installationen“, auf Seite 101.

Anpassen von Installationen mit der ESXi Image Builder CLI

Sie können ESXi Image Builder CLI dazu verwenden, ESXi-Installations-Images mit einem angepassten Satz von Updates, Patches und Treibern zu erstellen.

Die ESXi Image Builder CLI ist ein Satz von PowerShell-CLI-Befehlen, den Sie zur Erstellung eines ESXi-Installations-Images mit einem angepassten Satz von ESXi-Updates und -Patches verwenden können. Sie können auch Netzwerk- oder Speichertreiber von Drittanbietern hinzufügen, die zwischen vSphere-Versionen herausgegeben werden.

Sie können ein ESXi-Image, das mit Image Builder erstellt wurde, auf eine der folgenden Weisen bereitstellen:

- Indem Sie es auf eine Installations-DVD brennen.
- Über vCenter Server mithilfe der Funktion „Auto Deploy“.

Siehe „Verwenden von vSphere ESXi Image Builder“, auf Seite 149 und „Installieren von ESXi mithilfe von vSphere Auto Deploy“, auf Seite 76.

Grundlegendes zum ESXi -Testmodus und -Lizenzmodus

Mit dem Testmodus können Sie alle Funktionen von ESXi-Hosts kennenlernen. Im Testmodus sind die gleichen Funktionen wie mit einer vSphere Enterprise Plus-Lizenz verfügbar. Vor Ablauf des Testmodus müssen Sie Ihren Hosts eine Lizenz zuweisen, die alle genutzten Funktionen unterstützt.

Beispielsweise können Sie im Testmodus vSphere vMotion-Technologie, die vSphere HA-Funktion, die vSphere DRS-Funktion und andere Funktionen nutzen. Wenn Sie diese Funktionen weiter nutzen möchten, müssen Sie ihnen eine Lizenz zuweisen, die sie unterstützt.

Die installierbare Version von ESXi-Hosts wird immer im Testmodus installiert. ESXi Embedded wird von Ihrem Hardwareanbieter auf einem internen Speichergerät vorinstalliert. Es ist möglicherweise im Testmodus oder vorlizenziert.

Die Testperiode beträgt 60 Tage und beginnt mit dem Einschalten des ESXi-Host. Während der 60-tägigen Testphase können Sie jederzeit vom lizenzierten Modus in den Testmodus wechseln. Die in der Testperiode verfügbare Zeit wird um die bereits genutzte Zeit reduziert.

Angenommen, Sie haben einen ESXi-Host im Testmodus bereits seit 20 Tagen verwendet und weisen dann dem Host einen vSphere Standard Edition-Lizenzschlüssel zu. Wenn Sie den Host auf den Testmodus zurücksetzen, können Sie alle Funktionen des Hosts während der verbleibenden 40 Tage im Testmodus nutzen.

Informationen zur Lizenzierung für ESXi-Hosts finden Sie in der Dokumentation *vCenter Server und Hostverwaltung*.

Medienoptionen für das Starten des ESXi-Installationsprogramms

Das ESXi-Installationsprogramm muss für das System erreichbar sein, auf dem Sie ESXi installieren.

Für das ESXi-Installationsprogramm werden die folgenden Startmedien unterstützt:

- Starten von CD/DVD. Weitere Informationen hierzu finden Sie unter „Herunterladen und Brennen des ESXi-Installer-ISO-Images auf eine CD oder DVD“, auf Seite 42.
- Starten von einem USB-Flash-Laufwerk. Weitere Informationen hierzu finden Sie unter „Formatieren eines USB-Flash-Laufwerks für das Starten der ESXi-Installation oder des Upgrades“, auf Seite 43.
- Starten vom Netzwerk per PXE-Startvorgang. „Starten des ESXi-Installationsprogramms per PXE-Startvorgang“, auf Seite 46
- Starten von einem Remotespeicherort aus mit einer Remoteverwaltungsanwendung. Siehe „Verwenden von Anwendungen für die Remoteverwaltung“, auf Seite 54.

Herunterladen und Brennen des ESXi-Installer-ISO-Images auf eine CD oder DVD

Wenn Sie über keine ESXi-Installations-CD/DVD verfügen, können Sie eine erstellen.

Sie können auch ein Installer-ISO-Image erstellen, das ein benutzerdefiniertes Installationsskript enthält. Weitere Informationen hierzu finden Sie unter „Erstellen eines Installer-ISO-Images mit einem benutzerdefinierten Installations- oder Upgrade-Skript“, auf Seite 46.

Vorgehensweise

1. Laden Sie das ESXi-Installationsprogramm von der VMware-Website unter https://my.vmware.com/web/vmware/downloads herunter.

   ESXi ist unter „Datencenter- und Cloud-Infrastruktur“ aufgeführt

2. Bestätigen Sie, dass „md5sum“ korrekt ist.

   Weitere Informationen hierzu finden Sie auf der VMware-Website im Thema „Verwenden von MD5-Prüfsummen“ unter http://www.vmware.com/download/md5.html.

3. Brennen Sie das ISO-Image auf eine CD oder eine DVD.

Formatieren eines USB-Flash-Laufwerks für das Starten der ESXi-Installation oder des Upgrades

Sie können ein USB-Flash-Laufwerk für das Starten der ESXi-Installation oder des Upgrades formatieren.

Führen Sie den Vorgang auf einem Linux-Rechner mit einem Betriebssystem aus, in dem das USB-Flash-Laufwerk erkennt werden kann. In diesen Beispielen erkennt das Betriebssystem das USB-Flash-Laufwerk als `/dev/`*`sdb`*.

HINWEIS Die Datei `ks` mit dem Installationsskript darf sich nicht in dem USB-Flash-Laufwerk befinden, von dem aus die Installation oder das Upgrade gestartet wird.

Voraussetzungen

- Das ESXi-ISO-Image `VMware-VMvisor-Installer-`*`6.x.x-XXXXXX`*`.x86_64.iso`, einschließlich der Datei `isolinux.cfg`, wobei *`6.x.x`*die installierte ESXi-Version und *XXXXXX* die Build-Nummer des ISO-Image des Installationsprogramms ist
- Linux-Rechner mit Zugriff auf Syslinux Version 3.86 oder 4.03

Vorgehensweise

1 Wenn Ihr USB-Flash-Laufwerk nicht als `/dev/`*`sdb`* erkannt wird oder Sie nicht genau wissen, wie Ihr USB-Flash-Laufwerk erkannt wird, finden Sie es heraus.

  a Führen Sie dazu in der Befehlszeile den folgenden Befehl aus.

```
tail -f /var/log/messages
```

  Dieser Befehl zeigt aktuelle Protokollmeldungen an.

  b Schließen Sie Ihr USB-Flash-Laufwerk an.

  Es werden mehrere Meldungen angezeigt, die sich auf das USB-Flash-Laufwerk beziehen, und zwar in folgendem oder ähnlichem Format.

```
Oct 25 13:25:23 ubuntu kernel: [  712.447080] sd 3:0:0:0: [sdb] Attached SCSI removable
disk
```

  In diesem Beispiel gibt *sdb* das USB-Gerät an. Falls Ihr Gerät anderweitig identifiziert wird, verwenden Sie anstelle von *sdb* die betreffende Identifizierung.

2 Erstellen Sie eine Partitionstabelle auf dem USB-Flash-Gerät.

```
/sbin/fdisk /dev/sdb
```

  a Geben Sie `d` ein, um Partitionen zu löschen, bis alle Partitionen gelöscht sind.

  b Geben Sie `n` ein, um die primäre Partition 1 zu erstellen, die sich über die gesamte Festplatte erstreckt.

  c Geben Sie `t` ein, um für den Typ eine passende Einstellung für das Dateisystem FAT32 festzulegen, z. B. **`c`**.

  d Geben Sie `a` ein, um das aktive Flag auf Partition 1 zu setzen.

e Geben Sie p ein, um die Partitionstabelle auszugeben.

Das Ergebnis sollte dem folgenden Text ähneln:

```
Disk /dev/sdb: 2004 MB, 2004877312 bytes
255 heads, 63 sectors/track, 243 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes
   Device Boot      Start         End      Blocks   Id  System
/dev/sdb1             1           243      1951866  c   W95 FAT32 (LBA)
```

f Geben Sie w ein, um die Partitionstabelle zu schreiben und das Programm zu verlassen.

3 Formatieren Sie das USB-Flash-Laufwerk mit dem Dateisystem Fat32.

```
/sbin/mkfs.vfat -F 32 -n USB /dev/sdb1
```

4 Führen Sie die folgenden Befehle aus:

```
/path_to_syslinux-version_directory/syslinux-version/bin/syslinux /dev/sdb1
cat /path_to_syslinux-version_directory/syslinux-version/usr/share/syslinux/mbr.bin
> /dev/sdb
```

5 Mounten Sie das USB-Flash-Laufwerk.

```
mount /dev/sdb1 /usbdisk
```

6 Mounten Sie das ESXi-Installer-ISO-Image.

```
mount -o loop VMware-VMvisor-Installer-6.x.x-XXXXXX.x86_64.iso /esxi_cdrom
```

7 Kopieren Sie den Inhalt des ISO-Images nach `/usbdisk`.

```
cp -r /esxi_cdrom/* /usbdisk
```

8 Benennen Sie die Datei `isolinux.cfg` in `syslinx.cfg` um.

```
mv /usbdisk/isolinux.cfg /usbdisk/syslinux.cfg
```

9 Ändern Sie in der Datei `/usbdisk/syslinux.cfg` die Zeile `APPEND -c boot.cfg` in `APPEND -c boot.cfg -p 1`.

10 Bei Syslinux Version 4.03 ändern Sie `menu.c32`.

```
cp / path_to_syslinux directory/syslinux-4.03/usr/share/syslinux/menu.c32 /usbdisk/
```

11 Unmounten Sie das USB-Flash-Laufwerk.

```
umount /usbdisk
```

12 Unmounten Sie das ESXi-Installer-ISO-Image.

```
umount /esxi_cdrom
```

Das USB-Flash-Laufwerk kann das ESXi-Installationsprogramm starten.

Erstellen eines USB-Flash-Laufwerks für das Speichern des ESXi-Installations- oder -Upgrade-Skripts

Sie können ein USB-Flash-Laufwerk zum Speichern des ESXi-Installations- oder -Upgrade-Skripts verwenden, das während der Skriptinstallation bzw. des Skript-Upgrades von ESXi verwendet wird.

Wenn auf der Installationsmaschine mehrere USB-Flash-Laufwerke vorhanden sind, durchsucht die Installationssoftware alle angeschlossenen USB-Flash-Laufwerke nach dem Installations- oder Upgrade-Skript.

Die Anweisungen in diesem Verfahren setzen voraus, dass das USB-Flash-Laufwerk als `/dev/sdb` erkannt wird.

HINWEIS Die Datei `ks`, die das Installations- oder Upgrade-Skript enthält, darf sich nicht auf dem selben USB-Flash-Laufwerk befinden, von dem aus die Installation oder das Upgrade gestartet wird.

Voraussetzungen

- Linux-Maschine
- Installations- oder Upgrade-Skript für ESXi, die Kickstart-Datei `ks.cfg`
- USB-Flash-Laufwerk

Vorgehensweise

1 Schließen Sie das USB-Flash-Laufwerk an eine Linux-Maschine an, die auf das Installations- bzw. Upgrade-Skript zugreifen kann.

2 Erstellen Sie eine Partitionstabelle.

```
/sbin/fdisk /dev/sdb
```

a Geben Sie `d` ein, um Partitionen zu löschen, bis alle Partitionen gelöscht sind.

b Geben Sie `n` ein, um die primäre Partition 1 zu erstellen, die sich über die gesamte Festplatte erstreckt.

c Geben Sie `t` ein, um für den Typ eine passende Einstellung für das Dateisystem FAT32 festzulegen, z. B. **`c`**.

d Geben Sie `p` ein, um die Partitionstabelle auszugeben.

Das Ergebnis sollte dem folgenden Text ähneln:

```
Disk /dev/sdb: 2004 MB, 2004877312 bytes
255 heads, 63 sectors/track, 243 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes
   Device Boot      Start         End      Blocks   Id  System
/dev/sdb1             1           243      1951866  c   W95 FAT32 (LBA)
```

e Geben Sie `w` ein, um die Partitionstabelle zu schreiben und den Vorgang zu beenden.

3 Formatieren Sie das USB-Flash-Laufwerk mit dem Dateisystem Fat32.

```
/sbin/mkfs.vfat -F 32 -n USB /dev/sdb1
```

4 Mounten Sie das USB-Flash-Laufwerk.

```
mount /dev/sdb1 /usbdisk
```

5 Kopieren Sie das ESXi-Installationsskript auf das USB-Flash-Laufwerk.

```
cp ks.cfg /usbdisk
```

6 Unmounten Sie das USB-Flash-Laufwerk.

Das USB-Flash-Laufwerk enthält das Installations- oder das Upgrade-Skript für ESXi.

Weiter

Wenn Sie das ESXi-Installationsprogramm starten, verweisen Sie für das Installations- oder Upgrade-Skript auf den Speicherort des USB-Flash-Laufwerks. Siehe „Eingeben von Startoptionen zum Starten eines Installations- oder Upgrade-Skripts“, auf Seite 61 und „Grundlegendes zu PXE-Konfigurationsdateien“, auf Seite 50.

Erstellen eines Installer-ISO-Images mit einem benutzerdefinierten Installations- oder Upgrade-Skript

Sie können das standardmäßige ESXi-Installer-ISO-Image mit einem eigenen Installations- oder Upgrade-Skript anpassen. Diese Anpassung ermöglicht Ihnen die Durchführung einer skriptbasierten, unbeaufsichtigten Installation bzw. eines skriptbasierten, unbeaufsichtigten Upgrades, wenn Sie das resultierende Installer-ISO-Image starten.

Siehe auch „Grundlegendes zu Installations- und Upgrade-Skripts“, auf Seite 63 und „Grundlegendes zur Datei „boot.cfg““, auf Seite 72.

Voraussetzungen

- Linux-Maschine
- Das ESXi-ISO-Image `VMware-VMvisor-Installer-`*`6.x.x-XXXXXX`*`.x86_64.iso`, wobei *`6.x.x`* die Version von ESXi, die Sie installieren, und *`XXXXXX`* die Build-Nummer des Installer-ISO-Images ist.
- Ihr benutzerdefiniertes Installations- oder Upgrade-Skript, die Kickstart-Datei `ks_cust.cfg`.

Vorgehensweise

1. Laden Sie das ESXi-ISO-Image von der VMware-Website herunter.
2. Mounten Sie das ISO-Image in einen Ordner:

   ```
   mount -o loop VMware-VMvisor-Installer-6.x.x-XXXXXX.x86_64.iso /esxi_cdrom_mount
   ```

   `XXXXXX` ist die ESXi-Build-Nummer für die Version, die Sie installieren bzw. auf die Sie ein Upgrade ausführen.
3. Kopieren Sie den Inhalt von `cdrom` in einen anderen Ordner:

   ```
   cp -r /esxi_cdrom_mount /esxi_cdrom
   ```

4. Kopieren Sie die Kickstart-Datei nach `/esxi_cdrom`

   ```
   cp ks_cust.cfg /esxi_cdrom
   ```

5. (Optional) Ändern Sie die Datei `boot.cfg` mithilfe der Option `kernelopt` dahingehend, dass sie den Speicherort des Installations- oder Upgrade-Skripts angibt.

   Mit diesem Schritt wird die Installation bzw. das Upgrade automatisiert, da das Angeben der Kickstart-Datei während der Installation oder des Upgrades entfällt.
6. Neuerstellung des ISO-Images:

   ```
   mkisofs -relaxed-filenames -J -R -o custom_esxi.iso -b isolinux.bin -c boot.cat -no-emul-boot
   -boot-load-size 4 -boot-info-table /esxi_cdrom
   ```

Das ISO-Image enthält Ihr benutzerdefiniertes Installations- bzw. Upgrade-Skript.

Weiter

Installieren Sie ESXi aus dem ISO-Image.

Starten des ESXi-Installationsprogramms per PXE-Startvorgang

Sie verwenden PXE (Preboot Execution Environment) für den Startvorgang eines Hosts und um das ESXi-Installationsprogramm von einer Netzwerkschnittstelle zu starten.

ESXi 6.0 wird in einem ISO-Format verteilt, das für die Installation auf Flash-Arbeitsspeicher oder auf eine lokale Festplatte entwickelt wurde. Mithilfe von PXE können Sie die Dateien extrahieren und starten.

PXE verwendet Dynamic Host Configuration Protocol (DHCP) und Trivial File Transfer Protocol (TFTP), um ein Betriebssystem über ein Netzwerk zu starten.

Das Starten mit PXE setzt eine gewisse Netzwerkinfrastruktur und eine Maschine mit einem PXE-fähigen Netzwerkadapter voraus. Die meisten Maschinen, die ESXi ausführen können, verfügen über Netzwerkadapter, die PXE-Startvorgänge ermöglichen.

Hinweis Stellen Sie sicher, dass der vSphere Auto Deploy-Server über eine IPv4-Adresse verfügt. Das Starten per PXE-Startvorgang wird nur mit IPv4 unterstützt.

Grundlegendes zu TFTP-Server, PXELINUX und gPXE

Trivial File Transfer Protocol (TFTP) ähnelt dem FTP-Dienst und wird normalerweise nur für Netzwerkstartsysteme oder zum Laden der Firmware auf Netzwerkgeräten (z. B. Routern) verwendet.

Die meisten Linux-Distributionen enthalten eine Kopie des tftp-hpa-Servers. Wenn Sie eine unterstützte Lösung benötigen, erwerben Sie einen unterstützten TFTP-Server von einem Anbieter Ihrer Wahl.

Wenn Ihr TFTP-Server auf einem Microsoft Windows-Host ausgeführt werden soll, müssen Sie tftpd32 Version 2.11 oder höher verwenden. Weitere Informationen hierzu finden Sie unter http://tftpd32.jounin.net/. Frühere Versionen von tftpd32 sind nicht kompatibel mit PXELINUX und gPXE.

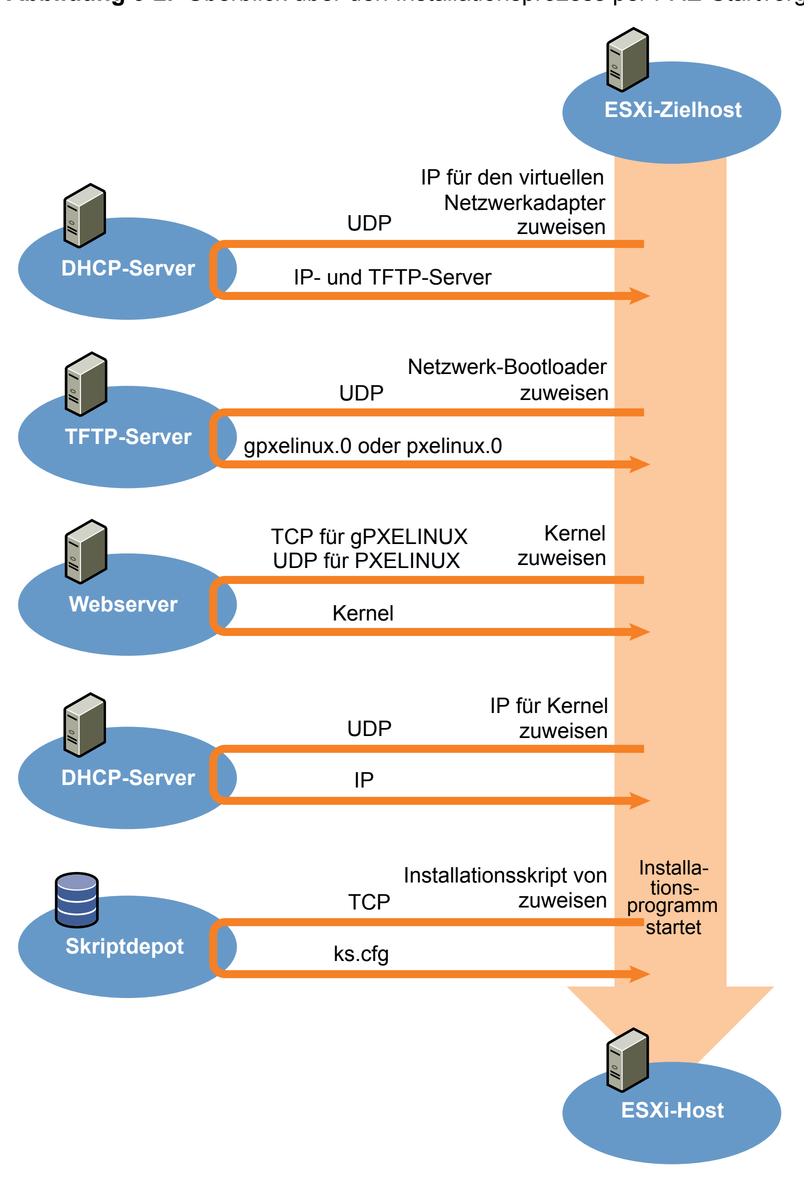
Sie können sich einen TFTP-Server auch von einem der verpackten Appliances auf dem VMware Marketplace beschaffen.

Die PXELINUX- und gPXE-Umgebungen ermöglichen das Starten des ESXi-Installationsprogramms durch die Zielmaschine. PXELINUX ist Teil des SYSLINUX-Pakets, das sich unter http://www.kernel.org/pub/linux/utils/boot/syslinux/ befindet. Viele Linux-Distributionen enthalten das Paket bereits. Viele Versionen von PXELINUX enthalten zudem gPXE. Einige Distributionen, wie z. B. Red Hat Enterprise Linux Version 5.3, enthalten frühere Versionen von PXELINUX, die gPXE nicht enthalten.

Wenn Sie gPXE nicht verwenden, können Probleme beim Starten des ESXi-Installationsprogramms auf einem stark ausgelasteten Netzwerk auftreten. TFTP ist manchmal unzuverlässig beim Übertragen großer Datenmengen. Wenn Sie PXELINUX ohne gPXE verwenden, werden die Binärdatei `pxelinux.0`, die Konfigurationsdatei, der Kernel und andere Dateien über TFTP übertragen. Wenn Sie gPXE verwenden, werden nur die Binärdatei `gpxelinux.0` und die Konfigurationsdatei über TFTP übertragen. Mit gPXE können Sie einen Webserver zum Übertragen des Kernels und anderer zum Starten des ESXi-Installationsprogramms erforderlichen Dateien verwenden.

Hinweis VMware testet den PXE-Startvorgang mit PXELINUX Version 3.86. Dies deutet jedoch nicht auf eine eingeschränkte Unterstützung hin. Wenden Sie sich an den jeweiligen Anbieter zwecks Unterstützung von Agenten von Drittanbietern, die Sie zum Einrichten Ihrer PXE-Startinfrastruktur verwenden.

Abbildung 3-2. Überblick über den Installationsprozess per PXE-Startvorgang



Beispiel-DHCP-Konfiguration

Der DHCP-Server muss zum Starten des ESXi-Installationsprogramms per PXE-Startvorgang die Adresse des TFTP-Servers sowie einen Zeiger auf das Verzeichnis `pxelinux.0` oder `gpxelinux.0` senden.

Der DHCP-Server wird von der Zielmaschine zum Abrufen einer IP-Adresse verwendet. Der DHCP-Server muss feststellen können, ob die Zielmaschine starten darf, und den Speicherort der PXELINUX-Binärdatei (die sich gewöhnlich auf einem TFTP-Server befindet) kennen. Beim Start der Zielmaschine sendet sie ein Paket über das Netzwerk, das diese Informationen anfordert, damit sie selbst starten kann. Der DHCP-Server antwortet.



Vorsicht Richten Sie keinen neuen DHCP-Server ein, wenn sich bereits einer in Ihrem Netzwerk befindet. Falls mehrere DHCP-Server auf die DHCP-Anforderungen reagieren, können Maschinen falsche oder widersprüchliche IP-Adressen abrufen oder nicht die richtigen Startinformationen erhalten. Sprechen Sie mit einem Netzwerkadministrator, bevor Sie einen DHCP-Server einrichten. Zur Unterstützung bei der Konfiguration von DHCP wenden Sie sich an den Hersteller Ihres DHCP-Servers.

Viele DHCP-Server können Hosts per PXE-Startvorgang starten. Wenn Sie eine Version von DHCP für Microsoft Windows verwenden, lesen Sie die DHCP-Serverdokumentation, um zu erfahren, wie die Argumente `next-server` und `filename` an die Zielmaschine übergeben werden.

gPXE-Beispiel

In diesem Beispiel wird gezeigt, wie ein ISC DHCP-Server der Version 3.0 für das Aktivieren von gPXE konfiguriert wird.

```
allow booting;
allow bootp;
# gPXE options
option space gpxe;
option gpxe-encap-opts code 175 = encapsulate gpxe;
option gpxe.bus-id code 177 = string;
class "pxeclients" {
   match if substring(option vendor-class-identifier, 0, 9) = "PXEClient";
   next-server TFTP server address;
   if not exists gpxe.bus-id {
      filename "/gpxelinux.0";
   }
}
subnet Network address netmask Subnet Mask {
   range Starting IP Address Ending IP Address;
}
```

Wenn eine Maschine einen Startvorgang per PXE versucht, stellt der DHCP-Server eine IP-Adresse und den Speicherort der Binärdatei `gpxelinux.0` auf dem TFTP-Server zur Verfügung. Die zugeordnete IP-Adresse befindet sich in dem Bereich, der im Subnetzabschnitt der Konfigurationsdatei definiert ist.

PXELINUX (ohne gPXE) Beispiel

In diesem Beispiel wird gezeigt, wie ein ISC DHCP-Server der Version 3.0 für das Aktivieren von PXELINUX konfiguriert wird.

```
#
# DHCP Server Configuration file.
#   see /usr/share/doc/dhcp*/dhcpd.conf.sample
#
ddns-update-style ad-hoc;
allow booting;
allow bootp;
class "pxeclients" {
   match if substring(option vendor-class-identifier, 0, 9) = "PXEClient";
   next-server xxx.xxx.xx.xx;
   filename = "pxelinux.0";
}
subnet 192.168.48.0 netmask 255.255.255.0 {
   range 192.168.48.100 192.168.48.250;
}
```

Wenn eine Maschine einen Startvorgang per PXE versucht, stellt der DHCP-Server eine IP-Adresse und den Speicherort der Binärdatei `pxelinux.0` auf dem TFTP-Server zur Verfügung. Die zugeordnete IP-Adresse befindet sich in dem Bereich, der im Subnetzabschnitt der Konfigurationsdatei definiert ist.

Grundlegendes zu PXE-Konfigurationsdateien

Die PXE-Konfigurationsdatei legt das Menü fest, das dem ESXi-Zielhost angezeigt wird, wenn er startet und den TFTP-Server kontaktiert. Für das Starten des ESXi-Installationsprogramms per PXE-Startvorgang benötigen Sie eine PXE-Konfigurationsdatei.

Der TFTP-Server überwacht ständig PXE-Clients im Netzwerk. Wenn er erkennt, dass ein PXE-Client PXE-Dienste anfordert, sendet er ein Netzwerkpaket, das ein Startmenü enthält, an den Client.

Erforderliche Dateien

Die PXE-Konfigurationsdatei muss die Pfade zu den folgenden Dateien enthalten:

- `mboot.c32` ist der Bootloader.
- `boot.cfg` ist die Bootloader-Konfigurationsdatei.

Siehe „Grundlegendes zur Datei „boot.cfg““, auf Seite 72.

Dateiname der PXE-Konfigurationsdatei

Wählen Sie als Dateinamen der PXE-Konfigurationsdatei eine der folgenden Optionen aus:

- `01-`*`mac-Adresse_von_ESXi-Zielhost`*. Beispiel: `01-23-45-67-89-0a-bc`
- Die IP-Adresse des ESXi-Zielhosts in hexadezimaler Schreibweise.
- `Standard`

Die anfängliche Startdatei `pxelinux.0` oder `gpxelinux.0` versucht, eine PXE-Konfigurationsdatei zu laden. Sie versucht es mit der MAC-Adresse des ESXi-Zielhosts, der der Code des ARP-Typs, der für Ethernet „01“ lautet, vorangestellt ist. Schlägt der Versuch fehl, versucht sie es mit der IP-Adresse des ESXi-Zielsystems in hexadezimaler Schreibweise. Letztendlich wird versucht, eine Datei namens `default` zu laden.

Speicherort der PXE-Konfigurationsdatei

Speichern Sie die Datei auf dem TFTP-Server im Verzeichnis `var/lib/tftpboot/pxelinux.cfg/`.

Sie können die Datei z. B. auf dem TFTP-Server unter `/tftpboot/pxelinux.cfg/01-00-21-5a-ce-40-f6` speichern. Die MAC-Adresse des Netzwerkadapters auf dem ESXi-Zielhost ist 00-21-5a-ce-40-f6.

Starten des ESXi-Installationsprogramms per PXE-Startvorgang unter Verwendung von PXELINUX und einer PXE-Konfigurationsdatei

Sie können einen TFTP-Server zum Starten des ESXi-Installationsprogramms per PXE-Startvorgang mithilfe von PXELINUX und einer PXE-Konfigurationsdatei verwenden.

Siehe auch „Grundlegendes zu Installations- und Upgrade-Skripts“, auf Seite 63 und „Grundlegendes zur Datei „boot.cfg““, auf Seite 72.

Voraussetzungen

Überprüfen Sie, ob Ihre Umgebung über die folgenden Komponenten verfügt:

- Das ISO-Image des ESXi-Installationsprogramms, das von der VMware-Website heruntergeladen wurde.
- TFTP-Server mit gPXE, der den PXE-Startvorgang unterstützt. Siehe „Grundlegendes zu TFTP-Server, PXELINUX und gPXE“, auf Seite 47.
- DHCP-Server, der für PXE-Startvorgänge konfiguriert ist. Siehe „Beispiel-DHCP-Konfiguration“, auf Seite 48.
- PXELINUX.

- Server mit einer Hardwarekonfiguration, die von Ihrer ESXi-Version unterstützt wird. Weitere Informationen finden Sie im VMware-Kompatibilitätshandbuch unter http://www.vmware.com/resources/compatibility/search.php.
- Netzwerksicherheitsrichtlinien zum Zulassen des TFTP-Datenverkehrs (UDP-Port 69)
- (Optional) Installationsskript, die Kickstart-Datei. Siehe „Grundlegendes zu Installations- und Upgrade-Skripts“, auf Seite 63.
- Netzwerkadapter mit PXE-Unterstützung auf dem Ziel-ESXi-Host
- IPv4-Netzwerk. IPv6 wird für die PXE-Startvorgänge nicht unterstützt.

In den meisten Fällen ist die Verwendung eines nativen VLANs sinnvoll. Um die VLAN-ID anzugeben, die mit dem PXE-Startvorgang verwendet wird, stellen Sie sicher, dass Ihre Netzwerkkarte die VLAN-ID-Spezifikation unterstützt.

Vorgehensweise

1 Erstellen Sie das Verzeichnis `/tftpboot/pxelinux.cfg` auf dem TFTP-Server.

2 Installieren Sie auf der Linux-Maschine PXELINUX.

   PXELINUX ist im Syslinux-Paket enthalten. Extrahieren Sie die Dateien, suchen Sie die Datei `pxelinux.0` und kopieren Sie sie in das Verzeichnis `/tftpboot` auf Ihrem TFTP-Server.

3 Konfigurieren Sie den DHCP-Server zum Senden der folgenden Informationen an jeden Clienthost:

   - Name oder IP-Adresse Ihres TFTP-Servers
   - Name der anfänglichen Startdatei, `pxelinux.0`

4 Kopieren Sie den Inhalt des ESXi-Installationsprogramm-Images in das Verzeichnis `/var/lib/tftpboot` des TFTP-Servers.

5 (Optional) Fügen Sie für eine Skriptinstallation in der `boot.cfg`-Datei die Option `kernelopt` in die Zeile nach dem Kernelbefehl ein, um den Speicherort des Installationsskripts anzugeben.

   Verwenden Sie den folgenden Code als Beispiel, wobei `XXX.XXX.XXX.XXX` die IP-Adresse des Servers ist, auf dem sich das Installationsskript befindet, und `esxi_ksFiles` das Verzeichnis, in dem sich die Datei `ks.cfg` befindet.

   ```
   kernelopt=ks=http://XXX.XXX.XXX.XXX/esxi_ksFiles/ks.cfg
   ```

6 Erstellen Sie eine PXE-Konfigurationsdatei.

   Diese Datei legt fest, wie der Host gestartet wird, wenn kein Betriebssystem verfügbar ist. Die PXE-Konfigurationsdatei referenziert die Startdateien. Verwenden Sie den folgenden Code als Beispiel, wobei `XXXXXX` die Build-Nummer des Images des ESXi-Installationsprogramms ist.

   ```
   DEFAULT menu.c32
   MENU TITLE ESXi-6.x.x-XXXXXX-full Boot Menu
   NOHALT 1
   PROMPT 0
   TIMEOUT 80
   LABEL install
     KERNEL mboot.c32
      APPEND -c location of boot.cfg
   MENU LABEL ESXi-6.x.x-XXXXXX-full ^Installer
   LABEL hddboot
    LOCALBOOT 0x80
    MENU LABEL ^Boot from local disk
   ```

7 Geben Sie die MAC-Adresse (Media Access Control) der Zielhostmaschine als Name der Datei an: `01-mac-Adresse_von_ESXi-Zielhost`.

   Beispiel: `01-23-45-67-89-0a-bc`.

8 Speichern Sie die PXE-Konfigurationsdatei unter `/tftpboot/pxelinux.cfg` auf dem TFTP-Server.

9 Starten Sie die Maschine mit dem Netzwerkadapter.

Starten des ESXi-Installationsprogramms per PXE-Startvorgang mithilfe von PXELINUX und der PXE-Konfigurationsdatei „isolinux.cfg“

Sie können das ESXi-Installationsprogramm per PXE-Startvorgang mithilfe von PXELINUX starten und die Datei „isolinux.cfg“ als PXE-Konfigurationsdatei verwenden.

Siehe auch „Grundlegendes zu Installations- und Upgrade-Skripts“, auf Seite 63 und „Grundlegendes zur Datei „boot.cfg““, auf Seite 72.

Voraussetzungen

Überprüfen Sie, ob Ihre Umgebung über die folgenden Komponenten verfügt:

- Das ISO-Image des ESXi-Installationsprogramms, das von der VMware-Website heruntergeladen wurde.
- TFTP-Server mit PXELINUX, der den PXE-Startvorgang unterstützt. Siehe „Grundlegendes zu TFTP-Server, PXELINUX und gPXE“, auf Seite 47.
- DHCP-Server, der für PXE-Startvorgänge konfiguriert ist. Siehe „Beispiel-DHCP-Konfiguration“, auf Seite 48.
- PXELINUX.
- Server mit einer Hardwarekonfiguration, die von Ihrer ESXi-Version unterstützt wird. Weitere Informationen finden Sie im VMware-Kompatibilitätshandbuch unter http://www.vmware.com/resources/compatibility/search.php.
- Netzwerksicherheitsrichtlinien zum Zulassen des TFTP-Datenverkehrs (UDP-Port 69)
- (Optional) Installationsskript, die Kickstart-Datei. Siehe „Grundlegendes zu Installations- und Upgrade-Skripts“, auf Seite 63.
- Netzwerkadapter mit PXE-Unterstützung auf dem Ziel-ESXi-Host
- IPv4-Netzwerk. IPv6 wird für die PXE-Startvorgänge nicht unterstützt.

In den meisten Fällen ist die Verwendung eines nativen VLANs sinnvoll. Um die VLAN-ID anzugeben, die mit dem PXE-Startvorgang verwendet wird, stellen Sie sicher, dass Ihre Netzwerkkarte die VLAN-ID-Spezifikation unterstützt.

Vorgehensweise

1 Erstellen Sie das Verzeichnis `/tftpboot/pxelinux.cfg` auf dem TFTP-Server.

2 Installieren Sie auf der Linux-Maschine PXELINUX.

   PXELINUX ist im Syslinux-Paket enthalten. Extrahieren Sie die Dateien, suchen Sie die Datei `pxelinux.0` und kopieren Sie sie in das Verzeichnis `/tftpboot` auf Ihrem TFTP-Server.

3 Konfigurieren Sie den DHCP-Server.

   Der DHCP-Server sendet die folgenden Informationen an Ihre Clienthosts:

   - Name oder IP-Adresse Ihres TFTP-Servers
   - Name der anfänglichen Startdatei, `pxelinux.0`

4 Kopieren Sie den Inhalt des ESXi-Installationsprogramm-Images in das Verzeichnis `/var/lib/tftpboot` des TFTP-Servers.

5 (Optional) Fügen Sie für eine Skriptinstallation in der `boot.cfg`-Datei die Option `kernelopt` in die nächste Zeile nach dem `kernel`-Befehl ein, um den Speicherort des Installationsskripts anzugeben.

   Im folgenden Beispiel ist *XXX.XXX.XXX.XXX* die IP-Adresse des Servers, auf dem sich das Installationsskript befindet.

```
kernelopt=ks=http://XXX.XXX.XXX.XXX/esxi_ksFiles/ks.cfg
```

6 Kopieren Sie die Datei `isolinux.cfg` vom ISO-Image des ESXi-Installationsprogramms in das Verzeichnis `/tftpboot/pxelinux.cfg`.

   Die Datei `isolinux.cfg` enthält den folgenden Code, bei dem `XXXXXX` die Build-Nummer des ESXi-Installationsprogramm-Images ist:

```
DEFAULT menu.c32
MENU TITLE ESXi-6.x.x-XXXXXX-full Boot Menu
NOHALT 1
PROMPT 0
TIMEOUT 80
LABEL install
  KERNEL mboot.c32
   APPEND -c location of boot.cfg
MENU LABEL ESXi-6.x.x-XXXXXX-full ^Installer
LABEL hddboot
 LOCALBOOT 0x80
 MENU LABEL ^Boot from local disk
```

7 Benennen Sie die Datei `isolinux.cfg` mit der MAC-Adresse der Zielhostmaschine um: `01-mac-Adresse_von_ESXi-Zielhost`. Beispiel: `01-23-45-67-89-0a-bc`

8 Starten Sie die Maschine mit dem Netzwerkadapter.

Starten des ESXi-Installationsprogramms per PXE-Startvorgang mithilfe von gPXE

Sie können das ESXi-Installationsprogramm per PXE-Startvorgang mithilfe von gPXE ausführen.

Siehe auch „Grundlegendes zu Installations- und Upgrade-Skripts“, auf Seite 63 und „Grundlegendes zur Datei „boot.cfg““, auf Seite 72.

Voraussetzungen

Überprüfen Sie, ob Ihre Umgebung über die folgenden Komponenten verfügt:

- Das ISO-Image des ESXi-Installationsprogramms, das von der VMware-Website heruntergeladen wurde
- HTTP-Webserver, auf den Ihre Ziel-ESXi-Hosts zugreifen können
- DHCP-Server, der für PXE-Startvorgänge konfiguriert ist: `/etc/dhcpd.conf` wird für Clienthosts mit einem TFTP-Server und der anfänglichen Startdatei `gpxelinux.0/undionly.kpxe` konfiguriert. Weitere Informationen hierzu finden Sie unter „Beispiel-DHCP-Konfiguration“, auf Seite 48.
- Server mit einer Hardwarekonfiguration, die von Ihrer ESXi-Version unterstützt wird. Weitere Informationen finden Sie im Hardware-Kompatibilitätshandbuch unter http://www.vmware.com/resources/compatibility/search.php.
- gPXELINUX
- (Optional) ESXi-Installationsskript. Weitere Informationen hierzu finden Sie unter „Grundlegendes zu Installations- und Upgrade-Skripts“, auf Seite 63.

In den meisten Fällen ist die Verwendung eines nativen VLANs sinnvoll. Wenn Sie die VLAN-ID angeben möchten, die mit dem PXE-Startvorgang verwendet wird, stellen Sie sicher, dass Ihre Netzwerkkarte die VLAN-ID-Spezifikation unterstützt.

Vorgehensweise

1 Kopieren Sie den Inhalt des ISO-Images des ESXi-Installationsprogramms in das Verzeichnis `/var/www/html` des HTTP-Servers.

2 Passen Sie die `boot.cfg`-Datei mit den Informationen für den HTTP-Server an.

   Verwenden Sie den folgenden Code als Beispiel, wobei *XXX.XXX.XXX.XXX* die IP-Adresse des HTTP-Servers ist. Die Zeile `kernelopt` ist optional. Verwenden Sie diese Option, um den Speicherort des Installationsskripts für eine Skriptinstallation anzugeben.

```
title=Loading ESX installer
kernel=http://XXX.XXX.XXX.XXX/tboot.b00
kernelopt=ks=http://XXX.XXX.XXX.XXX/esxi_ksFiles/ks.cfg
modules=http://XXX.XXX.XXX.XXX/b.b00 --- http://XXX.XXX.XXX.XXX/useropts.gz ---
http://XXX.XXX.XXX.XXX/k.b00 --- http://XXX.XXX.XXX.XXX/a.b00 ---
http://XXX.XXX.XXX.XXX/s.v00 --- http://XXX.XXX.XXX.XXX/weaselin.t00 ---
http://XXX.XXX.XXX.XXX/tools.t00 --- http://XXX.XXX.XXX.XXX/imgdb.tgz ---
http://XXX.XXX.XXX.XXX/imgpayld.tgz
```

3 Starten Sie den Host per gPXE-Startvorgang und drücken Sie Strg+B, um auf das GPT-Menü zuzugreifen.

4 Geben Sie die folgenden Befehle zum Starten mit dem ESXi-Installationsprogramm ein, wobei *XXX.XXX.XXX.XXX* die IP-Adresse des HTTP-Servers ist.

```
dhcp net0 ( if dchp is not set)
kernel -n mboot.c32 http://XXX.XXX.XXX.XXX/mboot.c32
imgargs mboot.c32 -c http://XXX.XXX.XXX.XXX/boot.cfg
boot mboot.c32
```

Installieren und Starten von ESXi mit Software FCoE

Sie können ESXi von einer FCoE LUN mit VMware Software-FCoE-Adaptern und Netzwerkadaptern mit FCoE-Auslagerungsfunktionen installieren und starten. Ihr Host benötigt keinen dedizierten FCoE HBA.

In der Dokumentation *vSphere-Speicher* finden Sie Informationen über die Installation und das Starten von ESXi mit Software FCoE.

Verwenden von Anwendungen für die Remoteverwaltung

Remotemanagement-Anwendungen ermöglichen Ihnen die Installation von ESXi auf Servermaschinen an Remotestandorten.

Zu den für die Installation unterstützten Remotemanagement-Anwendungen gehören HP Integrated Lights-Out (iLO), Dell Remote Access Card (DRAC), IBM Management Module (MM), und Remote Supervisor Adapter II (RSA II). Eine Liste der zurzeit unterstützten Servermodelle und Remotemanagement-Firmwareversionen finden Sie unter „Unterstützte Remotemanagement-Servermodelle und Firmware-Versionen“, auf Seite 23. Wenn Sie Unterstützung für Remotemanagement-Anwendungen benötigen, wenden Sie sich an Ihren Hersteller.

Sie können Remotemanagement-Anwendungen verwenden, um interaktive Installationen und Skriptinstallationen von ESXi remote durchzuführen.

Wenn Sie Remotemanagement-Anwendungen verwenden, um ESXi zu installieren, können bei ausgelasteten Systemen oder Netzwerken bei Verwendung der virtuellen CD Probleme mit beschädigten Dateien auftreten. Falls eine Remoteinstallation eines ISO-Images fehlschlägt, schließen Sie die Installation unter Verwendung des physischen CD-Mediums ab.

Erforderliche Informationen für die Installation von ESXi

Bei einer interaktiven Installation werden Sie vom System zur Angabe der erforderlichen Systeminformationen aufgefordert. Bei einer Skriptinstallation müssen Sie diese Informationen im Installationsskript eingeben.

Notieren Sie sich die während der Installation verwendeten Werte zur zukünftigen Verwendung. Diese Notizen sind nützlich, wenn Sie ESXi neu installieren müssen und Sie die Werte, die Sie ursprünglich ausgewählt haben, erneut verwenden möchten.

Tabelle 3-1. Erforderliche Informationen für die Installation von ESXi

Informationen	Erforderlich oder optional	Standard	Anmerkungen
Tastaturlayout	Erforderlich	U.S. English	
VLAN-ID	Optional	Keine	Bereich: 0 bis 4094
IP-Adresse	Optional	DHCP	Sie können zulassen, dass DHCP das Netzwerk während der Installation konfiguriert. Nach der Installation können sie die Netzwerkeinstellungen ändern.
Subnetzmaske	Optional	Kalkuliert auf Basis der IP-Adresse	
Gateway	Optional	Auf Basis der konfigurierten IP-Adresse und der Subnetzmaske	
primärem DNS	Optional	Auf Basis der konfigurierten IP-Adresse und der Subnetzmaske	
sekundärem DNS	Optional	Keine	
Hostname	Erforderlich für statische IP-Einstellungen	Keine	Der vSphere Web Client kann entweder den Hostnamen oder die IP-Adresse verwenden, um auf den ESXi-Host zuzugreifen.
Installationsspeicherort	Erforderlich	Keine	Muss mindestens 5 GB sein, wenn Sie die Komponenten auf einer einzelnen Festplatte installieren.
Migrieren Sie vorhandene ESXi-Einstellungen. Bestehenden VMFS-Datenspeicher übernehmen.	Erforderlich, wenn Sie ESXi auf einem Laufwerk mit einer vorhandenen ESXi-Installation installieren.	Keine	Wenn bereits eine ESXi 5.x-Installation vorhanden ist, bietet das ESXi-Installationsprogramm die Wahl zwischen dem Beibehalten oder dem Überschreiben des VMFS-Datenspeichers bei der Installation.
Root-Kennwort	Optional	Keine	Das Root-Kennwort muss zwischen 8 und 40 Zeichen lang sein. Weitere Informationen zu Kennwörtern finden Sie in der Dokumentation *vSphere-Sicherheit*.

Herunterladen des ESXi-Installationsprogramms

Laden Sie das Installationsprogramm für ESXi herunter.

Voraussetzungen

Erstellen Sie ein „Mein VMware"-Konto unter https://my.vmware.com/web/vmware/.

Vorgehensweise

1 Laden Sie das ESXi-Installationsprogramm von der VMware-Website unter https://my.vmware.com/web/vmware/downloads herunter.

   ESXi ist unter „Datencenter- und Cloud-Infrastruktur" aufgeführt

2 Bestätigen Sie, dass „md5sum" korrekt ist.

   Weitere Informationen hierzu finden Sie auf der VMware-Website im Thema „Verwenden von MD5-Prüfsummen" unter http://www.vmware.com/download/md5.html.

Installieren von ESXi 4

Sie können ESXi interaktiv mit einer Skriptinstallation oder mit vSphere Auto Deploy installieren.

Dieses Kapitel behandelt die folgenden Themen:

Interaktives Installieren von ESXi

Verwenden Sie für kleine Bereitstellungen von weniger als fünf Hosts die Option für eine interaktive Installation.

Bei einer typischen interaktiven Installation starten Sie das ESXi-Installationsprogramm und reagieren auf Aufforderungen des Installationsprogramms, um ESXi auf der lokalen Hostfestplatte zu installieren. Das Installationsprogramm formatiert und partitioniert die Zielfestplatte neu und installiert das ESXi-Boot-Image. Falls Sie ESXi nicht bereits auf der Zielfestplatte installiert haben, werden alle Daten auf dem Laufwerk überschrieben, einschließlich Hardwareanbieter- und Betriebssystempartitionen sowie zugeordnete Daten.

HINWEIS Um sicherzustellen, dass keine Daten verloren gehen, migrieren Sie die Daten auf eine andere Maschine, bevor Sie ESXi installieren.

Wenn Sie ESXi auf einer Festplatte installieren, auf der sich eine vorherige Installation von ESXi bzw. ESX oder ein VMFS-Datenspeicher befindet, bietet Ihnen das Installationsprogramm Upgrade-Optionen. Weitere Informationen finden Sie in der *vSphere-Upgrade*-Dokumentation.

Interaktives Installieren von ESXi

Sie können die ESXi-CD/-DVD oder ein USB-Flash-Laufwerk zum Installieren der ESXi-Software auf einer SAS-, SATA- oder SCSI-Festplatte oder einem USB-Laufwerk verwenden.

Voraussetzungen

- Das ESXi-Installations-ISO-Image muss sich an einem der folgenden Speicherorte befinden:
  - Auf CD oder DVD. Wenn Sie nicht über die Installations-CD bzw. -DVD verfügen, können Sie eine erstellen. Siehe „Herunterladen und Brennen des ESXi-Installer-ISO-Images auf eine CD oder DVD", auf Seite 42.

- Auf einem USB-Flash-Laufwerk. Siehe „Formatieren eines USB-Flash-Laufwerks für das Starten der ESXi-Installation oder des Upgrades“, auf Seite 43.

Hinweis Sie können das ESXi-Installationsprogramm per PXE-Startvorgang starten, um eine Interaktive oder Skriptinstallation zu starten. Siehe „Starten des ESXi-Installationsprogramms per PXE-Startvorgang“, auf Seite 46.

- Stellen Sie sicher, dass der Serverhardwaretaktgeber auf UTC eingestellt ist. Diese Einstellung befindet sich im System-BIOS.
- Stellen Sie sicher, dass eine Tastatur und ein Monitor an die Maschine angeschlossen sind, auf der die ESXi-Software installiert werden soll. Alternativ können Sie Sie ein Remoteverwaltungsanwendung verwenden. Weitere Informationen hierzu finden Sie unter „Verwenden von Anwendungen für die Remoteverwaltung“, auf Seite 54.
- Achten Sie darauf, die Verbindung zum Netzwerkspeicher zu trennen. Dies verkürzt die Zeit, die das Installationsprogramm zur Suche nach verfügbaren Festplattenlaufwerken benötigt. Beachten Sie, dass nach dem Trennen des Netzwerkspeichers alle Dateien auf den getrennten Festplatten nicht für die Installation zur Verfügung stehen.

  Trennen Sie keine LUN, die eine vorhandene ESX- oder ESXi-Installation enthält. Trennen Sie keinen VMFS-Datenspeicher, der die Servicekonsole einer vorhandenen ESX-Installation enthält. Diese Aktionen können sich auf das Ergebnis der Installation auswirken.
- Erfassen Sie die vom ESXi-Installationsassistenten erforderlichen Informationen. Siehe „Erforderliche Informationen für die Installation von ESXi“, auf Seite 55.
- Stellen Sie sicher, dass sich ESXi Embedded nicht auf der Maschine befindet. ESXi Installable und ESXi Embedded dürfen sich nicht auf demselben Host befinden.

Vorgehensweise

1. Legen Sie die CD/DVD des ESXi-Installationsprogramms in das CD-/DVD-Laufwerk ein oder schließen Sie das USB-Flash-Laufwerk des Installationsprogramms an und starten Sie die Maschine neu.
2. Stellen Sie im BIOS ein, dass vom CD-ROM-Gerät oder vom USB-Flash-Laufwerk gestartet wird.

   Informationen zum Ändern der Startreihenfolge finden Sie in der Dokumentation Ihres Hardwareherstellers.
3. Wählen Sie auf der Seite „Festplatte auswählen“ das Laufwerk aus, auf dem ESXi installiert werden soll, und drücken Sie die Eingabetaste.

   Drücken Sie F1, um Informationen zur ausgewählten Festplatte anzuzeigen.

   Hinweis Verlassen Sie sich beim Auswählen einer Festplatte nicht auf die Festplattereihenfolge in der Liste. Die Reihenfolge der Festplatten wird durch das BIOS festgelegt und erscheint möglicherweise durcheinander. Dies könnte beispielsweise bei Systemen auftreten, in denen ständig Laufwerke hinzugefügt und entfernt werden.

   Wenn Sie eine Festplatte auswählen, die Daten enthält, wird die Seite „Festplattenauswahl bestätigen“ angezeigt.

   Wenn Sie auf einer Festplatte installieren, auf dem sich eine vorherige ESXi- bzw. ESX-Installation oder ein VMFS-Datenspeicher befindet, bietet Ihnen das Installationsprogramm mehrere Möglichkeiten.

   Wichtig Wenn Sie eine vorhandene ESX/ESXi-Installation aktualisieren oder migrieren, finden Sie dazu weitere Informationen unter *vSphere-Upgrade*. Die Anweisungen im *Installations- und Einrichtungshandbuch für vSphere* beschränken sich auf eine Neuinstallation von ESXi.

Wenn Sie eine Festplatte auswählen, die zu einer Festplattengruppe für Virtual SAN gehört, hängt die resultierende Installation vom Festplattentyp und der Gruppengröße ab:

- Wenn Sie ein SSD-Laufwerk auswählen, werden das SSD-Laufwerk und alle untergeordneten Festplatten (HDD) in derselben Festplattengruppe gelöscht.
- Wenn Sie eine Magnetfestplatte (HDD) auswählen und sich in der Festplattengruppe mehr als zwei Festplatten befinden, wird nur die ausgewählte Festplatte gelöscht.
- Wenn Sie eine Magnetfestplatte (HDD) auswählen und sich in der Festplattengruppe maximal zwei Festplatten befinden, werden das SSD-Laufwerk und die ausgewählte Festplatte gelöscht.

Weitere Informationen zur Verwaltung von Virtual SAN-Festplattengruppen finden Sie in der Dokumentation *vSphere-Speicher*.

4 Wählen Sie den Tastaturtyp für den Host aus.

   Nach der Installation können Sie in der direkten Konsole den Tastaturtyp ändern.

5 Geben Sie das Root-Kennwort für den Host ein.

   Sie können das Kennwort leer lassen, geben Sie jedoch ein Kennwort zum Sichern des Systems beim ersten Start ein. Nach der Installation können Sie in der direkten Konsole das Kennwort ändern.

6 Drücken Sie zum Starten der Installation die Eingabetaste.

7 Entfernen Sie nach Abschluss der Installation die Installations-CD/ -DVD bzw. das USB-Flash-Laufwerk.

8 Drücken Sie die Eingabetaste, um den Host neu zu starten.

   Wenn Sie eine Neuinstallation durchführen oder einen vorhandenen VMFS-Datenspeicher überschreiben, werden während des Neustarts VFAT-Scratch- und VMFS-Partitionen auf der Hostfestplatte erstellt.

9 Legen Sie das erste Startlaufwerk als das Laufwerk fest, auf dem Sie ESXi in Schritt 3 installiert haben.

   Informationen zum Ändern der Startreihenfolge finden Sie in der Dokumentation Ihres Hardwareanbieters.

HINWEIS UEFI-Systeme benötigen möglicherweise zusätzliche Schritte, um das Startgerät einzustellen. Siehe „Host kann nicht gestartet werden, nachdem Sie ESXi im UEFI-Modus installiert haben“, auf Seite 183.

Nach Abschluss der Installation können Sie die vorhandenen VMFS-Daten auf den ESXi-Host migrieren.

Sie können einen einzelnen Computer von jedem ESXi-Image aus starten. Das Starten mehrerer Geräte über ein einzelnes gemeinsames ESXi-Image wird nicht unterstützt.

Weiter

Einrichten der grundlegenden Verwaltung und Netzwerkkonfiguration für ESXi. Weitere Informationen hierzu finden Sie unter Kapitel 6, „Nach der Installation und Einrichtung von ESXi“, auf Seite 201.

Installieren von ESXi auf einer Software-iSCSI-Festplatte

Beim Installieren von ESXi auf einer Software-iSCSI-Festplatte müssen Sie den qualifizierten iSCSI-Namen (IQN) des Ziels konfigurieren.

Während des Systemstarts führt das System einen so genannten Power-On Self Test (POST) durch und beginnt, die Adapter in der im System-BIOS angegebenen Reihenfolge zu starten. Wenn der iBFT-Adapter (iSCSI Boot Firmware Table) an die Reihe kommt, versucht der Adapter, eine Verbindung mit dem Ziel herzustellen, startet jedoch nicht über es. Siehe „Voraussetzungen“.

Wenn die Verbindung zum iSCSI-Ziel erfolgreich hergestellt wurde, speichert die iSCSI-Boot-Firmware die iSCSI-Startkonfiguration in der iBFT. Der nächste zu startende Adapter muss das ESXi-Installationsmedium sein, entweder ein gemountetes ISO-Image oder eine physische CD-ROM.

Voraussetzungen

- Stellen Sie sicher, dass der Ziel-IQN in der iBFT-BIOS-Parametereinstellung des Ziels konfiguriert ist. Diese Einstellung befindet sich im Option-ROM der Netzwerkkarte, die für die iSCSI-LUN verwendet werden soll. Weitere Informationen hierzu finden Sie in der Anbieterdokumentation für Ihr System.
- Deaktivieren Sie die iBFT-Adapteroption zum Starten über das ISCSI-Ziel. Diese Aktion ist notwendig, um sicherzugehen, dass anstatt des iSCSI-Ziels das ESXi-Installationsprogramm startet. Wenn Sie Ihr System starten, befolgen Sie die Aufforderung zum Anmelden bei Ihrem iBFT-Adapter und deaktivieren Sie die Option zum Starten über das iSCSI-Ziel. Weitere Informationen hierzu finden Sie in der Anbieterdokumentation für Ihr System und den iBFT-Adapter. Nach Abschluss der Installation können Sie die Option zum Starten über die LUN, auf der Sie ESXi installieren, erneut aktivieren.

Vorgehensweise

1. Starten Sie eine interaktive Installation von der ESXi-Installations-CD/-DVD oder dem ISO-Image aus.
2. Wählen Sie im Bildschirm „Festplatte auswählen“ das iSCSI-Ziel aus, das Sie in der iBFT-BIOS-Parametereinstellung des Ziels angegeben haben.

   Falls das Ziel nicht in diesem Menü erscheint, stellen Sie sicher, dass die TCP/IP- und die iSCSI-Initiator-IQN-Einstellungen korrekt sind. Überprüfen Sie die ACL (Access Control List) des Netzwerks und stellen Sie sicher, dass der Adapter über ausreichende Berechtigungen für den Zugriff auf das Ziel verfügt.
3. Folgen Sie den Eingabeaufforderungen, um die Installation abzuschließen.
4. Starten Sie den Host neu.
5. Geben Sie die BIOS-Konfiguration des iBFT-Adapters in den Host-BIOS-Einstellungen ein und ändern Sie den Adapterparameter, sodass vom iSCSI-Ziel gestartet wird.

   Weitere Informationen hierzu finden Sie in der Anbieterdokumentation für Ihr System.

Weiter

Aktivieren Sie die Option zum Starten über das iSCSI-Ziel auf dem iBFT-Adapter erneut, sodass das System von der LUN startet, auf der Sie ESXi installiert haben.

Installieren oder Upgraden von Hosts mithilfe eines Skripts

Mithilfe von automatischen Skriptinstallationen oder -Upgrades können Sie ESXi-Hosts schnell bereitstellen. Skriptinstallationen oder -Upgrades bieten eine effiziente Möglichkeit zum Bereitstellen mehrerer Hosts.

Das Installations- oder Upgrade-Skript enthält die Installationseinstellungen für ESXi. Sie können das Skript für alle Hosts anwenden, die eine ähnliche Konfiguration haben sollen.

Für Skriptinstallationen oder -Upgrades müssen Sie die unterstützten Befehle verwenden, um ein Skript zu erstellen. Sie können das Skript bearbeiten, um Einstellungen zu ändern, die für jeden einzelnen Host unterschiedlich sind.

Das Installations- oder Upgrade-Skript kann sich an einem der folgenden Speicherorte befinden:

- FTP-Server
- HTTP/HTTPS-Server
- NFS-Server
- USB-Flash-Laufwerk

- CD-ROM-Laufwerk

Vorgehensweisen für die Skriptinstallation

Sie können mit einem einzigen Skript ESXi auf mehreren Computern installieren oder ein separates Skript für jeden einzelnen Computer verwenden.

Weil sich Festplattennamen von Maschine zu Maschine unterscheiden, ist zum Beispiel eine der Einstellungen, die Sie in einem Skript konfigurieren möchten, die Auswahl der Festplatte, auf der Sie ESXi installieren.

Tabelle 4-1. Auswahlmöglichkeiten bei der Skriptinstallation

Option	Aktion
Installieren Sie bei mehreren Rechnern immer auf der ersten Festplatte.	Erstellen Sie ein einzelnes Skript.
Installieren Sie ESXi für jede Maschine auf einer anderen Festplatte.	Erstellen Sie mehrere Skripts.

Weitere Informationen zu den Befehlen, die zum Angeben der zu installierenden Festplatte erforderlich sind, finden Sie unter „Installation und Upgrade von Skriptbefehlen“, auf Seite 64.

Eingeben von Startoptionen zum Starten eines Installations- oder Upgrade-Skripts

Sie können ein Installations- oder Upgrade-Skript starten, indem Sie Start-Befehlszeilenoptionen in die Start-Befehlszeile des ESXi-Installationsprogramms eingeben.

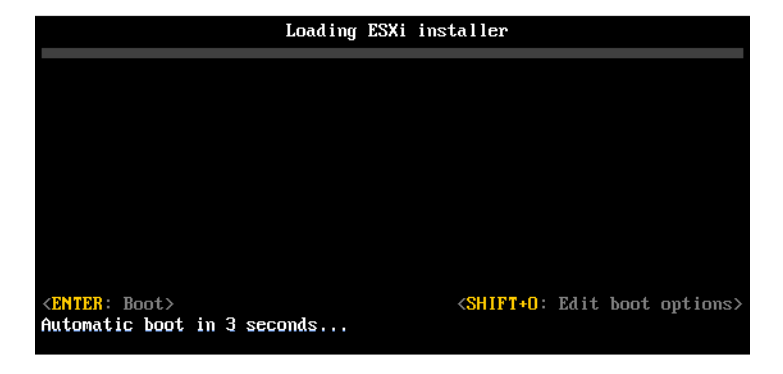
Beim Starten müssen Sie möglicherweise Optionen zum Aktivieren des Zugriffs auf die Kickstart-Datei angeben. Sie können Startoptionen eingeben, indem Sie im Bootloader Shift+O drücken. Für eine Installation per PXE-Startvorgang können Sie Optionen über die Zeile `kernelopts` der Datei `boot.cfg` übergeben. Siehe „Grundlegendes zur Datei „boot.cfg““, auf Seite 72 und „Starten des ESXi-Installationsprogramms per PXE-Startvorgang“, auf Seite 46.

Um den Speicherort des Installationsskripts anzugeben, legen Sie die Option `ks=`*`filepath`* fest, wobei *filepath* den Speicherort der Kickstart-Datei angibt. Andernfalls kann eine Skriptinstallation bzw. ein Skript-Upgrade nicht starten. Wenn `ks=`*`filepath`* ausgelassen wird, wird das Textinstallationsprogramm ausgeführt.

Unterstützte Startoptionen werden in „Startoptionen“, auf Seite 62 aufgelistet.

Vorgehensweise

1. Starten Sie den Host.
2. Wenn das Fenster des ESXi-Installationsprogramms erscheint, drücken Sie Umschalt+O, um die Startoptionen zu bearbeiten.



3 Geben Sie an der `runweasel`-Eingabeaufforderung **`ks=`*`Speicherort des Installationsskripts und die Start-Befehlszeilenoptionen`*** ein.

Beispiel: Startoption

Sie geben die folgenden Startoptionen ein:

```
ks=http://00.00.00.00/kickstart/ks-osdc-pdp101.cfg nameserver=00.00.0.0 ip=00.00.00.000 net-
mask=255.255.255.0 gateway=00.00.00.000
```

Startoptionen

Wenn Sie eine Skriptinstallation ausführen, müssen Sie möglicherweise beim Starten Optionen angeben, um auf die Kickstart-Datei zugreifen zu können.

Unterstützte Startoptionen

Tabelle 4-2. Startoptionen für die ESXi -Installation

Startoption	Beschreibung
`BOOTIF=`*`hwtype-MAC-Adresse`*	Ähnlich der Option `netdevice`, außer dass das PXELINUX-Format verwendet wird, wie in der Option IPAPPEND unter SYSLINUX auf der Website syslinux.zytor.com beschrieben.
`gateway=`*`IP-Adresse`*	Legt dieses Netzwerk-Gateway als Standard-Gateway für den Download des Installationsskripts und der Installationsmedien fest.
`ip=`*`IP-Adresse`*	Richtet eine statische IP-Adresse ein, die zum Herunterladen des Installationsskripts und der Installationsmedien verwendet wird. Hinweis: Das PXELINUX-Format für diese Option wird auch unterstützt. Weitere Informationen finden Sie unter der Option IPAPPEND unter SYSLINUX auf der Website syslinux.zytor.com.
`ks=cdrom:/`*`Pfad`*	Führt eine Skriptinstallation anhand des Skripts unter *Pfad* durch, das sich auf der CD im CD-ROM-Laufwerk befindet. Jede CD-ROM wird gemountet und so lange geprüft, bis die Datei, die dem Pfad entspricht, gefunden wird.
`ks=file://`*`Pfad`*	Führt eine Skriptinstallation anhand des Skripts unter *Pfad* aus.
`ks=`*`Protokoll`*`://`*`ServerPfad`*	Führt eine Skriptinstallation anhand eines Skripts aus, das sich im Netzwerk an der angegebenen URL befindet. *Protokoll* kann `http`, `https`, `ftp` oder `nfs` sein. Ein Beispiel für die Verwendung von NFS-Protokollen ist `ks=nfs://`*`Host`*`:`*`PortURL-Pfad`*. Das Format einer NFS-URL wird in RFC 2224 festgelegt.
`ks=usb`	Führt eine Skriptinstallation anhand eines Skripts auf einem angeschlossenen USB-Laufwerk aus. Sucht nach einer Datei namens `ks.cfg`. Die Datei muss sich im Stammverzeichnis des Laufwerks befinden. Falls mehrere USB-Flash-Laufwerke angeschlossen sind, werden sie so lange durchsucht, bis die Datei `ks.cfg` gefunden wird. Nur FAT16- und FAT32-Dateisysteme werden unterstützt.
`ks=usb:/`*`Pfad`*	Führt eine Skriptinstallation anhand der Skriptdatei mit dem angegebenen Pfad durch, die sich auf USB befindet.

Tabelle 4-2. Startoptionen für die ESXi -Installation (Fortsetzung)

Startoption	Beschreibung
`ksdevice=`*`Gerät`*	Versucht, einen Netzwerkadapter *Gerät* bei der Suche nach einem Installationsskript und Installationsmedium zu verwenden. Geben Sie dies als MAC-Adresse an, z. B. 00.50.56: C0: 00:01. Dieser Speicherort kann auch ein vmnicNN-Name sein. Sofern sie nicht angegeben wird und Dateien über das Netzwerk abgerufen werden müssen, wird der erste vom Installationsprogramm erkannte Netzwerkadapter verwendet, der angeschlossen ist.
`nameserver=`*`IP–Adresse`*	Gibt einen DNS-Server an, der zum Herunterladen des Installationsskripts und der Installationsmedien verwendet wird.
`netdevice=`*`Gerät`*	Versucht, einen Netzwerkadapter *Gerät* bei der Suche nach einem Installationsskript und Installationsmedium zu verwenden. Geben Sie dies als MAC-Adresse an, z. B. 00.50.56: C0: 00:01. Dieser Speicherort kann auch ein vmnicNN-Name sein. Sofern sie nicht angegeben wird und Dateien über das Netzwerk abgerufen werden müssen, wird der erste vom Installationsprogramm erkannte Netzwerkadapter verwendet, der angeschlossen ist.
`netmask=`*`Subnetzmaske`*	Gibt die Subnetzmaske für die Netzwerkkarte an, über die das Installationsskript und das Installationsmedium heruntergeladen wird.
`vlanid=`*`vlanid`*	Konfigurieren Sie die Netzwerkkarte, sodass sie auf dem angegebenen VLAN verwendet werden kann.

Grundlegendes zu Installations- und Upgrade-Skripts

Das Installations- bzw. Upgrade-Skript ist eine Textdatei, z. B. `ks.cfg`, die unterstützte Befehle enthält.

Der Befehlsabschnitt des Skripts enthält die ESXi-Installationsoptionen. Dieser Abschnitt ist zwingend. Er muss der erste Abschnitt im Skript sein.

Grundlegendes zum Standardinstallationsskript „ks.cfg“

Das ESXi-Installationsprogramm enthält ein Standardinstallationsskript, das eine Standardinstallation auf der ersten erkannten Festplatte durchführt.

Das Standardinstallationsskript `ks.cfg` befindet sich auf der anfänglichen RAM-Disk unter `/etc/vmware/weasel/ks.cfg`. Sie können den Speicherort der Standarddatei `ks.cfg` mithilfe der Startoption `ks=file://etc/vmware/weasel/ks.cfg` angeben. Siehe „Eingeben von Startoptionen zum Starten eines Installations- oder Upgrade-Skripts“, auf Seite 61.

Wenn Sie ESXi mithilfe des Skripts `ks.cfg` installieren, lautet das Standard-Root-Kennwort `mypassword`.

Sie können das Standardskript auf dem Installationsmedium nicht ändern. Nach der Installation können Sie vSphere Web Client verwenden, um sich am vCenter-Server, der den ESXi-Host verwaltet, anzumelden, und die Standardeinstellungen ändern.

Das Standardskript enthält folgende Befehle:

```
#
# Sample scripted installation file
#

# Accept the VMware End User License Agreement
vmaccepteula
```

```
# Set the root password for the DCUI and Tech Support Mode
rootpw mypassword

# Install on the first local disk available on machine
install --firstdisk --overwritevmfs

# Set the network to DHCP on the first network adapter
network --bootproto=dhcp --device=vmnic0

# A sample post-install script
%post --interpreter=python --ignorefailure=true
import time
stampFile = open('/finished.stamp', mode='w')
stampFile.write( time.asctime() )
```

Unterstützte Speicherorte für Installations- oder Upgrade-Skripts

Im Falle von Installationen und Upgrades, die per Skript durchgeführt wurden, kann das ESXi-Installationsprogramm von mehreren Speicherorten aus auf das Installations- bzw. Upgrade-Skript, das auch als Kickstart-Datei bezeichnet wird, zugreifen.

Die folgenden Speicherorte werden für Installations- oder Upgrade-Skripts unterstützt:

- CD/DVD. Weitere Informationen hierzu finden Sie unter „Erstellen eines Installer-ISO-Images mit einem benutzerdefinierten Installations- oder Upgrade-Skript“, auf Seite 46.
- USB-Flash-Laufwerk. Weitere Informationen hierzu finden Sie unter „Erstellen eines USB-Flash-Laufwerks für das Speichern des ESXi-Installations- oder -Upgrade-Skripts“, auf Seite 44.
- Ein Netzwerkspeicherort, auf den mithilfe der folgenden Protokolle zugegriffen werden kann: NFS, HTTP, HTTPS und FTP

Pfad des Installations- oder Upgrade-Skripts

Sie können den Pfad eines Installations- oder Upgrade-Skripts angeben.

`ks=http://XXX.XXX.XXX.XXX/kickstart/KS.CFG` ist der Pfad des ESXi-Installationsskripts, wobei*XXX.XXX.XXX.XXX*die IP-Adresse der Maschine ist, auf der sich das Skript befindet. Weitere Informationen hierzu finden Sie unter „Grundlegendes zu Installations- und Upgrade-Skripts“, auf Seite 63.

Zum Starten eines Installationsskripts aus einer interaktiven Installation müssen Sie die Option `ks=` manuell eingeben. Weitere Informationen hierzu finden Sie unter „Eingeben von Startoptionen zum Starten eines Installations- oder Upgrade-Skripts“, auf Seite 61.

Installation und Upgrade von Skriptbefehlen

Um das Standardinstallationsskript zu modifizieren, ein Skript zu aktualisieren oder ein eigenes Skript zu erstellen, verwenden Sie unterstützte Befehle. Verwenden Sie unterstützte Befehle im Installationsskript, das Sie mit einem Startbefehl angeben, wenn Sie das Installationsprogramm starten.

Um festzustellen, auf welcher Festplatte ESXi installiert oder aktualisiert werden soll, benötigt das Installationsskript einen der folgenden Befehle: `install`, `upgrade` oder `installorupgrade`. Der Befehl `install` erstellt die Standardpartitionen mit einem VMFS-Datenspeicher, der den gesamten Speicherplatz belegt, der nach der Erstellung der anderen Partitionen verfügbar ist.

accepteula/vmaccepteula (erforderlich)

Akzeptiert die ESXi-Lizenzvereinbarung.

clearpart (optional)

Löscht alle vorhandenen Partitionen auf der Festplatte. Setzt voraus, dass der Befehl `install` angegeben wird. Bearbeiten Sie den Befehl `clearpart` in Ihren vorhandenen Skripts mit Bedacht.

`--drives=`	Entfernt Partitionen auf den angegebenen Laufwerken.
`--alldrives`	Ignoriert die Bedingung`--drives=` und erlaubt das Löschen von Partitionen auf allen Laufwerken.
`--ignoredrives=`	Entfernt Partitionen auf allen außer den angegebenen Laufwerken. Erforderlich, es sei denn, das Flag `--drives=` oder `--alldrives` wurde angegeben.
`--overwritevmfs`	Erlaubt das Überschreiben von VMFS-Partitionen auf den angegebenen Laufwerken. Standardmäßig ist das Überschreiben von VMFS-Partitionen nicht erlaubt.
`--firstdisk=` ***`disk-type1`*** **`[`*`disk-type2`*`,...]`**	Partitioniert die erste erkannte geeignete Festplatte. Standardmäßig werden die geeigneten Festplatten in der folgenden Reihenfolge geordnet: 1 Lokal angehängter Speicher (`local`) 2 Netzwerkspeicher (`remote`) 3 USB-Festplatten (`usb`) Sie können die Reihenfolge der Festplatten durch eine kommagetrennte Liste ändern, die an das Argument angehängt wird. Wenn Sie eine Filterliste angeben, werden die Standardeinstellungen überschrieben. Sie können Filter kombinieren, um eine bestimmte Festplatte anzugeben. Dazu gehören `esx` für die erste Festplatte, auf der ESXi installiert ist, Modell- und Anbieterinformationen sowie der Name des VMkernel-Gerätetreibers. Wenn Sie beispielsweise eine Festplatte mit dem Modellnamen ST3120814A und alle Festplatten bevorzugen, die den mptsas-Treiber anstatt einer lokalen Festplatte verwenden, geben Sie als Argument `--firstdisk=ST3120814A,mptsas,local` an.

dryrun (optional)

Analysiert und überprüft das Installationsskript. Führt die Installation nicht aus.

Installieren

Gibt an, dass es sich um eine Neuinstallation handelt. Ersetzt den auslaufenden Befehl `autopart` in Skriptinstallationen von ESXi 4.1. Einer der Befehle `install`, `upgrade` oder `installorupgrade` ist erforderlich, um die Festplatte anzugeben, auf der ESXi installiert oder aktualisiert werden soll.

`--disk= oder --drive=`	Legt die zu partitionierende Festplatte fest. Im Befehl `--disk=`*`Festplattenname`* kann *Festplattenname* eine der folgenden Formen haben: ■ Pfad: `--disk=`*`/vmfs/devices/disks/mpx.vmhba1:C0:T0:L0`* ■ MPX-Name: `--disk=`*`mpx.vmhba1:C0:T0:L0`* ■ VML-Name: `--disk=`*`vml.000000034211234`* ■ vmkLUN UID: `--disk=`*`vmkLUN_UID`*

Die Formate der angenommenen Laufwerksnamen finden Sie unter „Festplattengerätenamen“, auf Seite 72.

--firstdisk= ***disk-type1*****,** **[*****disk-type2*****,...]**

Partitioniert die erste erkannte geeignete Festplatte. Standardmäßig werden die geeigneten Festplatten in der folgenden Reihenfolge geordnet:

1. Lokal angehängter Speicher (`local`)
2. Netzwerkspeicher (`remote`)
3. USB-Festplatten (`usb`)

Sie können die Reihenfolge der Festplatten durch eine kommagetrennte Liste ändern, die an das Argument angehängt wird. Wenn Sie eine Filterliste angeben, werden die Standardeinstellungen überschrieben. Sie können Filter kombinieren, um eine bestimmte Festplatte anzugeben, einschließlich `esx` für die erste Festplatte, auf der ESX installiert ist, sowie Modell- und Anbieterinformationen oder des Namens des VMkernel-Gerätetreibers. Wenn Sie beispielsweise eine Festplatte mit dem Modellnamen ST3120814A und alle Festplatten bevorzugen, die den mptsas-Treiber anstatt einer lokalen Festplatte verwenden, geben Sie als Argument `--firstdisk=ST3120814A,mptsas,local` an.

--ignoressd

Schließt Solid-State-Laufwerke aus der Partitionierung aus. Diese Option kann mit dem Befehl `install` und der Option `--firstdisk` verwendet werden. Diese Option hat Vorrang vor der Option `--firstdisk`. Bei der Verwendung der Option `--drive` oder `--disk` und der Befehle `upgrade` und `installorupgrade` ist sie nicht zulässig. Weitere Informationen zum Verhindern der Formatierung von SSD-Laufwerken während der automatischen Partitionierung finden Sie in der Dokumentation *vSphere-Speicher*.

--overwritevsan

Sie müssen die Option `--overwritevsan` verwenden, wenn Sie ESXi auf einer SSD- oder HDD-Festplatte in einer Virtual SAN-Festplattengruppe installieren. Wenn Sie diese Option verwenden und die ausgewählte Festplatte keine Virtual SAN-Partition aufweist, schlägt die Installation fehl. Wenn Sie ESXi auf einer Festplatte installieren, die zu einer Virtual SAN-Festplattengruppe gehört, hängt das Ergebnis von der ausgewählten Festplatte ab:

- Wenn Sie ein SSD-Laufwerk auswählen, werden das SSD-Laufwerk und alle untergeordneten Festplatten (HDD) in derselben Festplattengruppe gelöscht.
- Wenn Sie eine Magnetfestplatte (HDD) auswählen und sich in der Festplattengruppe mehr als zwei Festplatten befinden, wird nur die ausgewählte Festplatte gelöscht.
- Wenn Sie eine Magnetfestplatte (HDD) auswählen und sich in der Festplattengruppe maximal zwei Festplatten befinden, werden das SSD-Laufwerk und die ausgewählte Festplatte gelöscht.

Weitere Informationen zur Verwaltung von Virtual SAN-Festplattengruppen finden Sie in der Dokumentation *vSphere-Speicher*.

--overwritevmfs

Wird benötigt, um vor der Installation einen vorhandenen VMFS-Datenspeicher auf der Festplatte zu überschreiben.

--preservevmfs — Behält während der Installation einen vorhandenen VMFS-Datenspeicher auf der Festplatte bei.

--novmfsondisk — Verhindert, dass eine VMFS-Partition auf dieser Festplatte erstellt wird. Muss mit `--overwritevmfs` verwendet werden, wenn eine VMFS-Partition bereits auf der Festplatte vorhanden ist.

installorupgrade

Einer der Befehle `install`, `upgrade` oder `installorupgrade` ist erforderlich, um die Festplatte anzugeben, auf der ESXi installiert oder aktualisiert werden soll.

--disk= oder --drive= — Legt die zu partitionierende Festplatte fest. Im Befehl `--disk=`*`Festplattenname`* kann *Festplattenname* eine der folgenden Formen haben:

- Pfad: `--disk=`*`/vmfs/devices/disks/mpx.vmhba1:C0:T0:L0`*
- MPX-Name: `--disk=`*`mpx.vmhba1:C0:T0:L0`*
- VML-Name: `--disk=`*`vml.000000034211234`*
- vmkLUN UID: `--disk=`*`vmkLUN_UID`*

Die Formate der angenommenen Laufwerksnamen finden Sie unter „Festplattengerätenamen", auf Seite 72.

--firstdisk=
***disk-type1*,**
[*disk-type2*,...] — Partitioniert die erste erkannte geeignete Festplatte. Standardmäßig werden die geeigneten Festplatten in der folgenden Reihenfolge geordnet:

1. Lokal angehängter Speicher (`local`)
2. Netzwerkspeicher (`remote`)
3. USB-Festplatten (`usb`)

Sie können die Reihenfolge der Festplatten durch eine kommagetrennte Liste ändern, die an das Argument angehängt wird. Wenn Sie eine Filterliste angeben, werden die Standardeinstellungen überschrieben. Sie können Filter kombinieren, um eine bestimmte Festplatte anzugeben, einschließlich `esx` für die erste Festplatte, auf der ESX installiert ist, sowie Modell- und Anbieterinformationen oder des Namens des VMkernel-Gerätetreibers. Wenn Sie beispielsweise eine Festplatte mit dem Modellnamen ST3120814A und alle Festplatten bevorzugen, die den mptsas-Treiber anstatt einer lokalen Festplatte verwenden, geben Sie als Argument `--firstdisk=ST3120814A,mptsas,local` an.

--overwritevsan — Sie müssen die Option `--overwritevsan` verwenden, wenn Sie ESXi auf einer SSD- oder HDD-Festplatte in einer Virtual SAN-Festplattengruppe installieren. Wenn Sie diese Option verwenden und die ausgewählte Festplatte keine Virtual SAN-Partition aufweist, schlägt die Installation fehl. Wenn Sie ESXi auf einer Festplatte installieren, die zu einer Virtual SAN-Festplattengruppe gehört, hängt das Ergebnis von der ausgewählten Festplatte ab:

- Wenn Sie ein SSD-Laufwerk auswählen, werden das SSD-Laufwerk und alle untergeordneten Festplatten (HDD) in derselben Festplattengruppe gelöscht.
- Wenn Sie eine Magnetfestplatte (HDD) auswählen und sich in der Festplattengruppe mehr als zwei Festplatten befinden, wird nur die ausgewählte Festplatte gelöscht.

- Wenn Sie eine Magnetfestplatte (HDD) auswählen und sich in der Festplattengruppe maximal zwei Festplatten befinden, werden das SSD-Laufwerk und die ausgewählte Festplatte gelöscht.

Weitere Informationen zur Verwaltung von Virtual SAN-Festplattengruppen finden Sie in der Dokumentation *vSphere-Speicher*.

--overwritevmfs

Installieren Sie ESXi, wenn eine VMFS-Partition auf der Festplatte zur Verfügung steht, aber keine ESX- oder ESXi-Installation vorhanden ist. Wenn diese Option nicht vorhanden ist, schlägt das Installationsprogramm fehl, wenn eine VMFS-Partition auf der Festplatte zur Verfügung steht, aber keine ESX- oder ESXi-Installation vorhanden ist.

keyboard (optional)

Legt den Tastaturtyp für das System fest.

keyboardType

Legt die Tastaturzuordnung für den ausgewählten Tastaturtyp fest. *keyboardType* muss einer der folgenden Typen sein.

- Belgisch
- Brasilianisch
- Kroatisch
- Tschechoslowakisch
- Dänisch
- Standard
- Estnisch
- Finnisch
- Französisch
- Deutsch
- Griechisch
- Isländisch
- Italienisch
- Japanisch
- Lateinamerikanisch
- Norwegisch
- Polnisch
- Portugiesisch
- Russisch
- Slowenisch
- Spanisch
- Schwedisch
- Französisch (Schweiz)
- Deutsch (Schweiz)

- Türkisch
- US Dvorak
- Ukrainisch
- Großbritannien

serialnum oder vmserialnum (optional)

Auslaufend in ESXi 5.0.x, unterstützt in ESXi 5.1. Konfiguriert die Lizenzierung. Wenn nicht angegeben, erfolgt die ESXi-Installation im Testmodus.

--esx=<license-key>	Gibt den zu verwendenden vSphere-Lizenzschlüssel an. Das Format besteht aus fünf Gruppen mit je fünf Zeichen (XXXXX-XXXXX-XXXXX-XXXXX-XXXXX).

network (optional)

Gibt eine Netzwerkadresse für das System an.

`--bootproto=[dhcp|static]`	Gibt an, ob die Netzwerkeinstellungen von DHCP abgerufen oder manuell festgelegt werden sollen.
`--device=`	Gibt entweder die MAC-Adresse der Netzwerkkarte oder den Gerätenamen im Format `vmnicNN` an, wie z. B. `vmnic0`. Diese Option bezieht sich auf das Uplink-Gerät für den virtuellen Switch.
`--ip=`	Legt eine IP-Adresse für die zu installierende Maschine im Format `xxx.xxx.xxx.xxx` fest. Dies ist für die Option `--bootproto=static` erforderlich und wird ansonsten ignoriert.
`--gateway=`	Legt das Standard-Gateway als IP-Adresse im Format `xxx.xxx.xxx.xxx` fest. Wird im Zusammenhang mit der Option `--bootproto=static` verwendet.
`--nameserver=`	Legt den primären Namenserver als IP-Adresse fest. Wird im Zusammenhang mit der Option `--bootproto=static` verwendet. Lassen Sie diese Option weg, falls Sie nicht vorhaben, DNS zu verwenden. Für die Option `--nameserver` können zwei IP-Adressen angegeben werden. Beispiel: `--nameserver="10.126.87.104[,10.126.87.120]"`
`--netmask=`	Legt die Subnetzmaske des installierten Systems im Format `255.xxx.xxx.xxx` fest. Wird im Zusammenhang mit der Option `--bootproto=static` verwendet.
`--hostname=`	Legt den Hostnamen für das installierte System fest.
`--vlanid=` ***`vlanid`***	Gibt das VLAN des Systems an. Wird entweder mit der Option `--bootproto=dhcp` oder `--bootproto=static` verwendet. Legen Sie den Wert auf eine Ganzzahl zwischen 1 und 4096 fest.
`--addvmportgroup=(0|1)`	Gibt an, ob die VM-Netzwerkportgruppe, die von virtuelle Maschinen verwendet wird, hinzugefügt werden soll. Der Standardwert ist 1.

paranoid (optional)

Sorgt dafür, dass Warnmeldungen zum Abbruch der Installation führen. Wenn Sie diesen Befehl auslassen, werden Warnmeldungen protokolliert.

part oder partition (optional)

Erstellt auf dem System einen zusätzlichen VMFS-Datenspeicher. Es kann nur ein Datenspeicher pro Festplatte erstellt werden. Kann nicht auf derselben Festplatte wie der `install`-Befehl verwendet werden. Es kann nur eine Partition pro Festplatte angegeben werden. Diese muss eine VMFS-Partition sein.

`Datenspeichername`	Gibt an, wo die Partition gemountet werden soll.
`--ondisk= oder --on-drive=`	Gibt die Festplatte oder das Laufwerk an, wo die Partition erstellt werden soll.
`--firstdisk=` ***`disk-type1,`*** **`[`*`disk-type2`*`,...]`**	Partitioniert die erste erkannte geeignete Festplatte. Standardmäßig werden die geeigneten Festplatten in der folgenden Reihenfolge geordnet: 1 Lokal angehängter Speicher (`local`) 2 Netzwerkspeicher (`remote`) 3 USB-Festplatten (`usb`) Sie können die Reihenfolge der Festplatten durch eine kommagetrennte Liste ändern, die an das Argument angehängt wird. Wenn Sie eine Filterliste angeben, werden die Standardeinstellungen überschrieben. Sie können Filter kombinieren, um eine bestimmte Festplatte anzugeben, einschließlich `esx` für die erste Festplatte, auf der ESX installiert ist, sowie Modell- und Anbieterinformationen oder des Namens des VMkernel-Gerätetreibers. Wenn Sie beispielsweise eine Festplatte mit dem Modellnamen ST3120814A und alle Festplatten bevorzugen, die den mptsas-Treiber anstatt einer lokalen Festplatte verwenden, geben Sie als Argument `--firstdisk=ST3120814A,mptsas,local` an.

reboot (optional)

Startet die Maschine nach Abschluss der Skriptinstallation neu.

`<--noeject>`	Nach der Installation wird die CD nicht ausgeworfen.

rootpw (erforderlich)

Legt das Root-Kennwort für das System fest.

`--iscrypted`	Legt fest, dass das Kennwort verschlüsselt ist.
`Kennwort`	Legt das Kennwort fest.

Aktualisieren

Einer der Befehle `install`, `upgrade` oder `installorupgrade` ist erforderlich, um die Festplatte anzugeben, auf der ESXi installiert oder aktualisiert werden soll.

`--disk= oder --drive=`	Legt die zu partitionierende Festplatte fest. Im Befehl `--disk=`*`Festplattenname`* kann *Festplattenname* eine der folgenden Formen haben: ■ Pfad: `--disk=`*`/vmfs/devices/disks/mpx.vmhba1:C0:T0:L0`* ■ MPX-Name: `--disk=`*`mpx.vmhba1:C0:T0:L0`* ■ VML-Name: `--disk=`*`vml.000000034211234`* ■ vmkLUN UID:`--disk=`*`vmkLUN_UID`*

	Die Formate der angenommenen Laufwerksnamen finden Sie unter „Festplattengerätenamen“, auf Seite 72.
--firstdisk= ***disk-type1*****,** **[*****disk-type2*****,...]**	Partitioniert die erste erkannte geeignete Festplatte. Standardmäßig werden die geeigneten Festplatten in der folgenden Reihenfolge geordnet: 1 Lokal angehängter Speicher (`local`) 2 Netzwerkspeicher (`remote`) 3 USB-Festplatten (`usb`) Sie können die Reihenfolge der Festplatten durch eine kommagetrennte Liste ändern, die an das Argument angehängt wird. Wenn Sie eine Filterliste angeben, werden die Standardeinstellungen überschrieben. Sie können Filter kombinieren, um eine bestimmte Festplatte anzugeben, einschließlich `esx` für die erste Festplatte, auf der ESX installiert ist, sowie Modell- und Anbieterinformationen oder des Namens des VMkernel-Gerätetreibers. Wenn Sie beispielsweise eine Festplatte mit dem Modellnamen ST3120814A und alle Festplatten bevorzugen, die den mptsas-Treiber anstatt einer lokalen Festplatte verwenden, geben Sie als Argument `--firstdisk=ST3120814A,mptsas,local` an.

%include oder include (optional)

Gibt ein anderes zu analysierendes Installationsskript an. Dieser Befehl wird ähnlich wie ein mehrzeiliger Befehl behandelt, er akzeptiert jedoch nur ein Argument.

Dateiname	Beispiel: `%include part.cfg`

%pre (optional)

Gibt ein Skript an, das vor der Evaluierung der Kickstart-Konfiguration ausgeführt werden soll. Sie können es z. B. verwenden, um Dateien zur Aufnahme in die Kickstart-Datei zu generieren.

--interpreter =[python|busybox]	Legt den zu verwendenden Interpreter fest. Die Standardeinstellung ist „busybox“.

%post (optional)

Führt das angegebene Skript nach Abschluss der Paketinstallation aus. Wenn Sie mehrere `%post`-Abschnitte festlegen, werden sie in der Reihenfolge ausgeführt, in der sie im Installationsskript angegeben sind.

--interpreter =[python|busybox]	Legt den zu verwendenden Interpreter fest. Die Standardeinstellung ist „busybox“.
--timeout=secs	Legt eine Zeitüberschreitung für das Ausführen des Skripts fest. Falls die Ausführung des Skripts nicht abgeschlossen ist, wenn die Zeitüberschreitung eintritt, wird es automatisch beendet.
--ignorefailure =[true|false]	Bei Angabe von „true“ wird die Installation auch dann als erfolgreich angesehen, wenn das `%post`-Skript fehlerhaft beendet wurde.

%firstboot

Erstellt ein `init`-Skript, das nur während des ersten Startvorgangs ausgeführt wird. Das Skript hat keinen Einfluss auf spätere Startvorgänge. Wenn Sie mehrere `%firstboot`-Abschnitte festlegen, werden sie in der Reihenfolge ausgeführt, in der sie in der Kickstart-Datei angegeben sind.

HINWEIS Sie können die Semantik des `%firstboot`-Skripts erst dann prüfen, wenn das System zum ersten Mal gestartet wird. Ein `%firstboot`-Skript enthält möglicherweise potenziell katastrophale Fehler, die erst nach Abschluss der Installation ersichtlich sind.

`--interpreter`
`=[python|busybox]`

Legt den zu verwendenden Interpreter fest. Die Standardeinstellung ist „busybox“.

HINWEIS Sie können die Semantik des `%firstboot`-Skripts erst dann prüfen, wenn das System zum ersten Mal gestartet wird. Wenn das Skript Fehler enthält, sind diese erst nach Abschluss der Installation ersichtlich.

Festplattengerätenamen

Die Installationsskriptbefehle `install`, `upgrade` und `installorupgrade` erfordern die Verwendung von Festplattengerätenamen.

Tabelle 4-3. Festplattengerätenamen

Formatieren	Beispiel	Beschreibung
VML	vml.00025261	Der Gerätename, wie vom VMkernel gemeldet
MPX	mpx.vmhba0:C0:T0:L0	Der Gerätename

Grundlegendes zur Datei „boot.cfg“

Die Bootloader-Konfigurationsdatei `boot.cfg` gibt den Kernel, die Kerneloptionen und die Boot-Module an, die der Bootloader `mboot.c32` in einer ESXi-Installation verwendet.

Die Datei `boot.cfg`, die im ESXi-Installationsprogramm enthalten ist. Sie können die Zeile `kernelopt` der Datei `boot.cfg` ändern, um den Speicherort eines Installationsskripts anzugeben oder andere Startoptionen zu übergeben.

Die Datei `boot.cfg` weist das folgende Format auf:

```
# boot.cfg -- mboot configuration file
#
# Any line preceded with '#' is a comment.

title=STRING
kernel=FILEPATH
kernelopt=STRING
modules=FILEPATH1 --- FILEPATH2... --- FILEPATHn

# Any other line must remain unchanged.
```

Die Befehle in der Datei `boot.cfg` werden zum Konfigurieren des Bootloaders verwendet.

Tabelle 4-4. Befehle in der Datei `boot.cfg` .

Befehl	Beschreibung
`title=`*`ZEICHENFOLGE`*	Legt den Titel des Bootloaders auf *`ZEICHENFOLGE`* fest.
`kernel=`*`DATEIPFAD`*	Legt den Kernelpfad auf *`DATEIPFAD`* fest.
`kernelopt=`*`ZEICHENFOLGE`*	Fügt *`ZEICHENFOLGE`* den Kernel-Startoptionen hinzu.
`modules=`*`DATEIPFAD1 --- DATEIPFAD2... --- DATEIPFADn`*	Listet die zu ladenden Module auf, getrennt durch drei Striche (`---`).

Siehe „Erstellen eines Installer-ISO-Images mit einem benutzerdefinierten Installations- oder Upgrade-Skript“, auf Seite 46, „Starten des ESXi-Installationsprogramms per PXE-Startvorgang unter Verwendung von PXELINUX und einer PXE-Konfigurationsdatei“, auf Seite 50, „Starten des ESXi-Installationsprogramms per PXE-Startvorgang mithilfe von PXELINUX und der PXE-Konfigurationsdatei „isolinux.cfg““, auf Seite 52 und „Starten des ESXi-Installationsprogramms per PXE-Startvorgang“, auf Seite 46.

Installieren oder Durchführen eines Upgrades von ESXi von einer CD oder DVD mithilfe eines Skripts

Sie können von einem CD-ROM- oder DVD-ROM-Laufwerk aus mithilfe eines Skripts, das die Installations- oder Upgrade-Optionen festlegt, ESXi installieren oder ein Upgrade davon durchführen.

Sie können das Installations- oder Upgrade-Skript starten, indem Sie beim Starten des Hosts eine Startoption eingeben. Sie können auch ein Installer-ISO-Image erstellen, das das Installationsskript enthält. Mit einem Installer-ISO-Image können Sie eine skriptbasierte, unbeaufsichtigte Installation durchführen, wenn Sie das resultierende Installer-ISO-Image starten. Siehe „Erstellen eines Installer-ISO-Images mit einem benutzerdefinierten Installations- oder Upgrade-Skript“, auf Seite 46.

Voraussetzungen

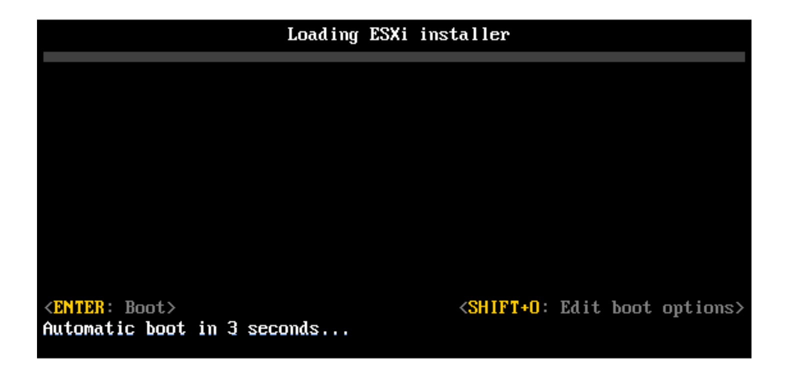
Bevor Sie die Installation oder das Upgrade per Skript ausführen, stellen Sie sicher, dass die folgenden Voraussetzungen erfüllt sind:

- Das System, auf dem Sie das Produkt installieren oder ein Upgrade davon durchführen, erfüllt die Hardwareanforderungen. Siehe „Hardwareanforderungen für ESXi“, auf Seite 21.
- Die ISO-Datei des ESXi-Installationsprogramms befindet sich auf einer Installations-CD oder -DVD. Siehe „Herunterladen und Brennen des ESXi-Installer-ISO-Images auf eine CD oder DVD“, auf Seite 42.
- Das System kann auf das Standardinstallations- oder -Upgrade-Skript (`ks.cfg`) oder ein benutzerdefiniertes Installations- oder -Upgrade-Skript zugreifen. Siehe „Grundlegendes zu Installations- und Upgrade-Skripts“, auf Seite 63.
- Sie haben einen Startbefehl ausgewählt, um die Installation oder das Upgrade per Skript auszuführen. Siehe „Eingeben von Startoptionen zum Starten eines Installations- oder Upgrade-Skripts“, auf Seite 61. Eine vollständige Liste der Startbefehle finden Sie unter „Startoptionen“, auf Seite 62.

Vorgehensweise

1 Starten Sie das ESXi-Installationsprogramm vom lokalen CD-ROM- oder DVD-ROM-Laufwerk aus.

2 Wenn das Fenster des ESXi-Installationsprogramms erscheint, drücken Sie Umschalt+O, um die Startoptionen zu bearbeiten.



3 Geben Sie eine Boot-Option ein, die das Standard-Installations- oder Upgrade-Skript bzw. ein von Ihnen erstelltes Installations- oder Upgrade-Skript aufruft.

   Die Startoption hat das Format `ks=`.

4 Drücken Sie die Eingabetaste.

Die Installation, das Upgrade bzw. die Migration wird anhand der von Ihnen angegebenen Optionen ausgeführt.

Installieren oder Durchführen eines Upgrades von ESXi von einem USB-Flash-Laufwerk mithilfe eines Skripts

Sie können von einem USB-Flash-Laufwerk aus mithilfe eines Skripts, das die Installations- oder Upgrade-Optionen festlegt, ESXi installieren oder ein Upgrade davon durchführen.

Unterstützte Startoptionen werden in „Startoptionen“, auf Seite 62 aufgelistet.

Voraussetzungen

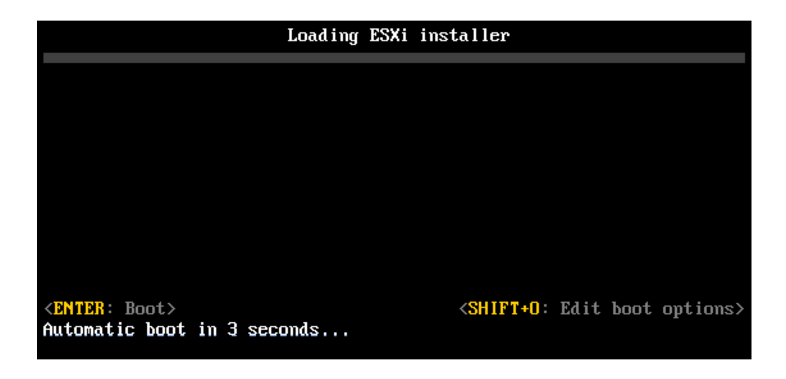
Bevor Sie die Installation oder das Upgrade per Skript ausführen, stellen Sie sicher, dass die folgenden Voraussetzungen erfüllt sind:

- Das System, auf dem Sie ESXi installieren oder aktualisieren, erfüllt die Hardwareanforderungen für die Installation bzw. das Upgrade. Siehe „Hardwareanforderungen für ESXi“, auf Seite 21.
- Die ESXi-Installer-ISO-Datei befindet sich auf einem startfähigen USB-Flash-Laufwerk. Siehe „Formatieren eines USB-Flash-Laufwerks für das Starten der ESXi-Installation oder des Upgrades“, auf Seite 43.
- Das System kann auf das Standardinstallations- oder -Upgrade-Skript (`ks.cfg`) oder ein benutzerdefiniertes Installations- oder -Upgrade-Skript zugreifen. Siehe „Grundlegendes zu Installations- und Upgrade-Skripts“, auf Seite 63.
- Sie haben eine Startoption ausgewählt, um die Installation, das Upgrade oder die Migration per Skript auszuführen. Siehe „Eingeben von Startoptionen zum Starten eines Installations- oder Upgrade-Skripts“, auf Seite 61.

Vorgehensweise

1 Starten Sie das ESXi-Installationsprogramm vom USB-Flash-Laufwerk aus.

2 Wenn das Fenster des ESXi-Installationsprogramms erscheint, drücken Sie Umschalt+O, um die Startoptionen zu bearbeiten.



3 Geben Sie eine Boot-Option ein, die das Standard-Installations- oder Upgrade-Skript bzw. ein von Ihnen erstelltes Installations- oder Upgrade-Skript aufruft.

   Die Startoption hat das Format `ks=`.

4 Drücken Sie die Eingabetaste.

Die Installation, das Upgrade bzw. die Migration wird anhand der von Ihnen angegebenen Optionen ausgeführt.

Ausführen einer Skriptinstallation oder eines Upgrades von ESXi durch Starten des Installationsprogramms per PXE-Startvorgang

ESXi 6.0 bietet viele Optionen zum Starten des Installationsprogramms per PXE-Startvorgang und zum Verwenden eines Installations- oder eines Upgrade-Skripts.

- Weitere Informationen zur Einrichtung einer PXE-Infrastruktur finden Sie unter „Starten des ESXi-Installationsprogramms per PXE-Startvorgang“, auf Seite 46.
- Weitere Informationen über das Erstellen und Auffinden eines Installationsskripts finden Sie unter „Grundlegendes zu Installations- und Upgrade-Skripts“, auf Seite 63.
- Weitere Informationen über bestimmte Prozeduren zum Starten des ESXi-Installationsprogramms per PXE-Startvorgang und zum Verwenden eines Installationsskripts finden Sie in den folgenden Themen:
  - „Starten des ESXi-Installationsprogramms per PXE-Startvorgang mithilfe von PXELINUX und der PXE-Konfigurationsdatei „isolinux.cfg““, auf Seite 52
  - „Starten des ESXi-Installationsprogramms per PXE-Startvorgang unter Verwendung von PXELINUX und einer PXE-Konfigurationsdatei“, auf Seite 50
  - „Starten des ESXi-Installationsprogramms per PXE-Startvorgang mithilfe von gPXE“, auf Seite 53
- Weitere Informationen über die Verwendung von vSphere Auto Deploy zum Durchführen einer Skriptinstallation per PXE-Startvorgang finden Sie unter„Installieren von ESXi mithilfe von vSphere Auto Deploy“, auf Seite 76.

Installieren von ESXi mithilfe von vSphere Auto Deploy

Mithilfe von vSphere Auto Deploy können Sie Hunderte von physischen Hosts mit ESXi-Software bereitstellen.

Mit Auto Deploy können erfahrene Systemadministratoren große Bereitstellungen effizient verwalten. Hosts werden über ein Netzwerk von einem zentralen Auto Deploy-Server aus gestartet. Hosts können wahlweise mit einem Hostprofil eines Referenzhosts konfiguriert werden. Das Hostprofil kann so eingerichtet werden, dass der Benutzer zur Eingabe aufgefordert wird. Nach Abschluss des Startvorgangs und der Konfiguration werden die Hosts durch vCenter Server wie andere ESXi-Hosts verwaltet.

Auto Deploy kann auch für statusfreies Caching und statusorientierte Installationen verwendet werden.

WICHTIG Auto Deploy erfordert eine sichere Trennung zwischen dem Produktionsnetzwerk und den Verwaltungs- oder Bereitstellungsnetzwerken, wie unter „Auto Deploy-Sicherheitsüberlegungen“, auf Seite 126 beschrieben. Die Verwendung von Auto Deploy ohne diese Trennung ist unsicher.

Statusfreies Caching
Standardmäßig speichert Auto Deploy die ESXi-Konfiguration bzw. den ESXi-Status nicht auf der Hostfestplatte. Stattdessen definiert ein Image-Profil das Image, mit dem der Host bereitgestellt wird, und andere Hostattribute werden durch Hostprofile verwaltet. Ein Host, der Auto Deploy für statusfreies Caching verwendet, muss nach wie vor mit dem Auto Deploy-Server und dem vCenter Server verbunden werden.

Statusorientierte Installationen
Sie können einen Host mit Auto Deploy bereitzustellen und den Host so einrichten, dass er das Image auf der Festplatte speichert. Bei nachfolgenden Startvorgängen wird der Host von der Festplatte aus gestartet.

Grundlegendes zu vSphere Auto Deploy

vSphere Auto Deploy kann Hunderte von physischen Hosts mit ESXi-Software bereitstellen. Sie können angeben, welches Image bereitgestellt werden soll und welche Hosts mit dem Image bereitgestellt werden sollen. Optional können Sie die Hostprofile, die auf die Hosts angewendet werden sollen, und einen vCenter Server-Speicherort (Ordner oder Cluster) für jeden Host angeben.

Einführung in Auto Deploy

Wenn Sie einen physischen Host starten, der für Auto Deploy eingerichtet ist, verwendet Auto Deploy eine PXE-Startvorgangsinfrastruktur in Verbindung mit vSphere-Hostprofilen, um diesen Host bereitzustellen und anzupassen. Auf dem Host selbst wird kein Status gespeichert. Stattdessen verwaltet der Auto Deploy-Server die Statusinformationen für jeden Host.

Statusinformationen für ESXi -Hosts

Auto Deploy speichert die Informationen für die bereitzustellenden ESXi-Hosts an verschiedenen Speicherorten. Die Informationen über den Speicherort der Image-Profile und Hostprofile wird anfänglich in den Regeln angegeben, die die Maschinen den Image-Profilen und Hostprofilen zuordnen.

Tabelle 4-5. Auto Deploy speichert Informationen zur Bereitstellung

Informationstyp	Beschreibung	Informationsquelle
Image-Status	Die ausführbare Software zur Ausführung auf einem ESXi-Host	Image-Profil, erstellt mit Image Builder PowerCLI.
Konfigurationsstatus	Die konfigurierbaren Einstellungen, die festlegen, wie der Host konfiguriert wird, z. B. virtuelle Switches und ihre Einstellungen, Treibereinstellungen, Startparameter usw	Hostprofil, das über die Benutzeroberfläche des Hostprofils erstellt wurde. Kommt oft von einem Vorlagen-Host.

Tabelle 4-5. Auto Deploy speichert Informationen zur Bereitstellung (Fortsetzung)

Informationstyp	Beschreibung	Informationsquelle
Status „Dynamisch“	Der Laufzeitstatus, der von der laufenden Software generiert wird, z. B. generierte private Schlüssel oder Laufzeitdatenbanken	Hostarbeitsspeicher, während des Startvorgangs verloren gegangen
Zustand der virtuellen Maschine	Die virtuellen Maschinen, die auf einem Host gespeichert sind, und Autostartinformationen für virtuelle Maschinen (nur bei nachfolgenden Startvorgängen)	Die VM-Informationen, die vom vCenter Server gesendet werden, müssen verfügbar sein, um Auto Deploy mit Informationen zur virtuellen Maschine zu versorgen.
Benutzereingabe	Der Status basiert auf der Benutzereingabe. So kann beispielsweise eine IP-Adresse, die der Benutzer beim Systemstart angibt, nicht automatisch in das Hostprofil aufgenommen werden.	Hostanpassungsdaten, gespeichert vom vCenter Server während des ersten Startvorgangs Sie können ein Hostprofil erstellen, das für bestimmte Werte eine Benutzereingabe erfordert. Wenn Auto Deploy ein Hostprofil anwendet, das vom Benutzer bereitgestellte Informationen erfordert, wird der Host in den Wartungsmodus versetzt. Verwenden Sie die Benutzeroberfläche für Hostprofile, um die Übereinstimmung von Hostprofilen zu prüfen, und antworten Sie auf die Aufforderung zum Anpassen des Hosts.

Auto Deploy-Architektur

Die Auto Deploy-Infrastruktur besteht aus mehreren Komponenten.

Weitere Informationen erhalten Sie im Video zur Auto Deploy-Architektur.



Auto Deploy-Architektur (http://link.brightcove.com/services/player/bcpid2296383276001?bctid=ref:video_auto_deploy_architecture)

Abbildung 4-1. vSphere Auto Deploy-Architektur

Auto Deploy PowerCLI
Hostprofile und Hostanpassung
Benutzeroberfläche für Hostprofile
Regel-Engine
Image Builder PowerCLI
Image-Profile
Auto Deploy-Server (Webserver)
Abrufen von vordefinierten Image-Profilen und VIBs
Plug-In
Host-profil-Engine
ESXi-Host
HTTP-Abruf von Images/VIBs und Hostprofilen (iPXE-Start und Update)
VIBs und Image-Profile
öffentliches Depot

Auto Deploy-Server

Server-Images und Hostprofile auf ESXi-Hosts

Auto Deploy-Regel-Engine

Sendet Informationen an den Auto Deploy-Server darüber, welches Image-Profil und welches Hostprofil für welchen Host bereitgestellt werden sollen. Administratoren verwenden die Auto Deploy PowerCLI zur Definition der Regeln, die den Hosts Image-Profile und Hostprofile zuweisen.

Image-Profile

Definieren Sie den VIB-Satz, mit dem die ESXi-Hosts gestartet werden sollen.

- VMware und VMware-Partner stellen Image-Profile und VIBs in öffentlichen Depots zur Verfügung. Verwenden Sie Image Builder PowerCLI zur Untersuchung des Depots und die Auto Deploy-Regel-Engine zur Festlegung, welches Image-Profil welchem Host zugewiesen werden soll.
- VMware-Kunden können ein benutzerdefiniertes Image-Profil auf Basis der öffentlichen Image-Profile und VIBs im Depot erstellen und dieses Image-Profil dem Host zuweisen. Siehe „Verwenden von vSphere ESXi Image Builder“, auf Seite 149.

Hostprofile

Definieren Sie eine maschinenspezifische Konfiguration, wie z. B. ein Netzwerk- oder Speicher-Setup. Erstellen Sie Hostprofile mithilfe der Benutzeroberfläche für Hostprofile. Sie können ein Hostprofil für einen Referenzhost erstellen und dieses Hostprofil auf andere Hosts in Ihrer Umgebung anwenden, um eine konsistente Konfiguration herzustellen.

Hostanpassung

Speichert Informationen, die der Benutzer angibt, wenn Hostprofile auf den Host angewendet werden. Die Hostanpassung kann möglicherweise eine IP-Adresse oder andere Informationen enthalten, die der Benutzer für diesen Host angegeben hat. Siehe „Hostanpassung im vSphere Web Client", auf Seite 118.

In früheren Versionen von Auto Deploy wurde die Hostanpassung „Antwortdatei" genannt.

Regeln und Regelsätze

Sie legen das Verhalten des Auto Deploy-Servers mithilfe eines Satzes von Regeln fest, die in der PowerCLI erstellt werden. Die Auto Deploy-Regel-Engine prüft den Regelsatz auf übereinstimmende Hostmuster, um die Elemente (Image-Profil, Hostprofil oder Speicherort von vCenter Server) festzulegen, mit denen jeder Host bereitgestellt werden soll.

Basierend auf den Attributen des Hosts ordnet die Regel-Engine den Hosts Software- und Konfigurationseinstellungen zu. Sie können beispielsweise Image-Profile oder Hostprofile auf zwei Clustern von Hosts bereitstellen, indem Sie zwei Regeln erstellen, die jeweils mit der Netzwerkadresse eines der Cluster übereinstimmen.

Im Falle von Hosts, die noch nicht zu einem vCenter Server-System hinzugefügt wurden, stimmt sich der Auto Deploy-Server mit der Regel-Engine ab, bevor Image-Profile, Hostprofile und Informationen zum Speicherort der Bestandsliste bereitgestellt werden. Bei von einem vCenter Server-System verwalteten Hosts werden das Image-Profil, das Hostprofil und der Speicherort der Bestandsliste verwendet, die vCenter Server im Hostobjekt gespeichert hat. Wenn Sie Änderungen an Regeln vornehmen, können Sie mithilfe von Auto Deploy-PowerCLI-cmdlets die Regelübereinstimmung testen und reparieren. Wenn Sie die Regelübereinstimmung für einen Host reparieren, werden das Image-Profil dieses Hosts und die Hostprofil-Zuweisungen aktualisiert.

Die Regel-Engine enthält Regeln und Regelsätze.

Regeln

Regeln können einer Gruppe von Hosts Image-Profile und Hostprofile zuweisen oder den Speicherort (Ordner oder Cluster) eines Hosts auf dem vCenter Server-Zielsystem festlegen. Eine Regel kann Zielhosts anhand der MAC-Startadresse, der SMBIOS-Informationen, der BIOS-UUID, des Anbieters, des Modells oder der festen DHCP-IP-Adresse identifizieren. In den meisten Fällen gelten die Regeln für mehrere Hosts. Sie erstellen Regeln mithilfe von Auto Deploy PowerCLI-cmdlets. Nachdem Sie eine Regel erstellt haben, müssen Sie sie zu einem Regelsatz hinzufügen. Nur zwei Regelsätze, der aktive Regelsatz und der Arbeitsregelsatz, werden unterstützt. Eine Regel kann zu beiden Sätzen (Standardeinstellung) oder nur zum Arbeitsregelsatz gehören. Nachdem Sie eine Regel zum Regelsatz hinzugefügt haben, können Sie die Regel nicht mehr ändern. Kopieren Sie stattdessen die Regel und ersetzen Sie Teile oder Muster in der Kopie.

Aktiver Regelsatz

Wenn ein neu gestarteter Host eine Anforderung für ein Image-Profil an den Auto Deploy-Server sendet, prüft der Auto Deploy-Server den aktiven Regelsatz auf übereinstimmende Regeln. Das Image-Profil, das Hostprofil und der Speicherort der vCenter Server-Bestandsliste, die durch übereinstimmen-

de Regeln zugeordnet werden, werden dann verwendet, um den Host zu starten. Wenn durch die Regeln mehrere Elemente des gleichen Typs zugeordnet wurden, verwendet der Auto Deploy-Server das Element, das als erstes im Regelsatz vorkommt.

Arbeitsregelsatz

Mithilfe des Arbeitsregelsatzes können Sie Änderungen an Regeln testen, bevor Sie die Änderungen aktivieren. Sie können beispielsweise die Auto Deploy PowerCLI-cmdlets zum Prüfen der Übereinstimmung mit dem Arbeitsregelsatz verwenden. Der Test überprüft, ob die von einem vCenter Server-System verwalteten Hosts die Regeln des Arbeitsregelsatzes einhalten. Standardmäßig fügen cmdlets die Regel zum Arbeitsregelsatz hinzu und aktivieren die Regeln. Verwenden Sie den Parameter `NoActivate`, um eine Regel nur zum Arbeitsregelsatz hinzuzufügen.

Sie verwenden den folgenden Workflow mit Regeln und Regelsätzen.

1 Nehmen Sie Änderungen am Arbeitsregelsatz vor.

2 Verwenden Sie cmdlets, die die Regeln des Arbeitsregelsatzes auf einen Host anwenden, um sicherzustellen, dass alles ordnungsgemäß funktioniert.

3 Definieren und testen Sie die Regeln im Arbeitsregelsatz neu.

4 Aktivieren Sie die Regeln im Arbeitsregelsatz.

   Wenn Sie eine Regel hinzufügen und den Parameter `NoActivate` nicht angeben, werden alle Regeln aktiviert, die sich zurzeit im Arbeitsregelsatz befinden. Sie können einzelne Regeln nicht aktivieren.

Weitere Informationen dazu finden Sie in der PowerCLI-Befehlszeilenhilfe und unter „Verwalten von Auto Deploy mithilfe von PowerCLI-cmdlets“, auf Seite 93.

Auto Deploy-Startvorgang

Wenn Sie einen Host starten, den Sie mit vSphere Auto Deploy bereitstellen bzw. erneut bereitstellen möchten, liefert die Auto Deploy-Infrastruktur das Image-Profil und optional ein Hostprofil und einen Speicherort für vCenter Server.

Der Startvorgang unterscheidet sich zwischen Hosts, die noch nicht mit Auto Deploy (erster Start) bereitgestellt wurden, und Hosts, die mit Auto Deploy bereitgestellt und einem vCenter Server-System (nachfolgender Start) hinzugefügt wurden.

Voraussetzungen für den ersten Start

Sie müssen vor einem ersten Startvorgang das System einrichten. Das Einrichten umfasst die folgenden Aufgaben, die unter „Vorbereitung für vSphere Auto Deploy“, auf Seite 87 detaillierter erläutert werden.

- Richten Sie einen DHCP-Server ein, der jedem Host beim Start eine IP-Adresse zuweist und den Host auf den TFTP-Server verweist, von dem der iPXE-Bootloader heruntergeladen wird.
- Stellen Sie sicher, dass der Auto Deploy-Server über eine IPv4-Adresse verfügt. Das Starten per PXE-Startvorgang wird nur mit IPv4 unterstützt.
- Identifizieren Sie ein Image-Profil, das auf eine der folgenden Arten verwendet werden soll.
  - Wählen Sie in einem öffentlichen Depot ein ESXi-Image-Profil aus.
  - (Optional) Erstellen Sie mithilfe der Image Builder PowerCLI ein benutzerdefiniertes Image-Profil und platzieren Sie es in einem Depot, auf das der Auto Deploy-Server zugreifen kann. Das Image-Profil muss ein Basis-ESXi-VIB enthalten.
- (Optional) Wenn sich ein Referenzhost in Ihrer Umgebung befindet, exportieren Sie das Hostprofil des Referenzhosts und definieren Sie eine Regel, die das Hostprofil auf einen oder mehrere Hosts anwendet. Siehe „Einrichten eines Auto Deploy-Referenzhosts“, auf Seite 110.

- Geben Sie Regeln für das Bereitstellen des Hosts an und fügen Sie die Regeln dem aktiven Regelsatz hinzu.

Überblick über den ersten Start

Wenn ein Host, der noch nicht mit vSphere Auto Deploy bereitgestellt wurde, startet (erster Start), interagiert er mit mehreren Auto Deploy-Komponenten.

1. Wenn der Administrator einen Host einschaltet, startet der Host eine PXE-Boot-Sequenz.

   Der DHCP-Server weist dem Host eine IP-Adresse zu und instruiert den Host, den TFTP-Server zu kontaktieren.

2. Der Host kontaktiert den TFTP-Server und lädt die iPXE-Datei (ausführbarer Bootloader) und eine iPXE-Konfigurationsdatei herunter.

3. iPXE beginnt mit der Ausführung.

   Die Konfigurationsdatei weist den Host an, eine HTTP-Startanforderung an den Auto Deploy-Server zu senden. Die HTTP-Anforderung enthält Hardware- und Netzwerkinformationen.

4. Im Gegenzug führt der Auto Deploy-Server die folgenden Aufgaben aus:

   a. Fragt die Regel-Engine nach Informationen über den Host ab.

   b. Streamt die im Image-Profil angegebenen Komponenten, das optionale Hostprofil und optionale Informationen zum Speicherort von vCenter Server.

5. Der Host startet unter Verwendung des Image-Profils.

   Falls der Auto Deploy-Server ein Hostprofil bereitgestellt hat, wird das Hostprofil auf den Host angewendet.

6. Auto Deploy fügt den Host zum vCenter Server-System hinzu, bei dem Auto Deploy registriert ist.

   a. Wenn eine Regel einen Zielordner oder einen Cluster auf dem vCenter Server-System angibt, wird der Host in diesem Ordner oder Cluster platziert. Der Zielordner muss sich in einem Datencenter befinden.

   b. Wenn keine Regel vorhanden ist, die den Speicherort einer vCenter Server-Bestandsliste angibt, fügt Auto Deploy den Host zum ersten Datencenter hinzu, das auf der Benutzeroberfläche des vSphere Web Client angezeigt wird.

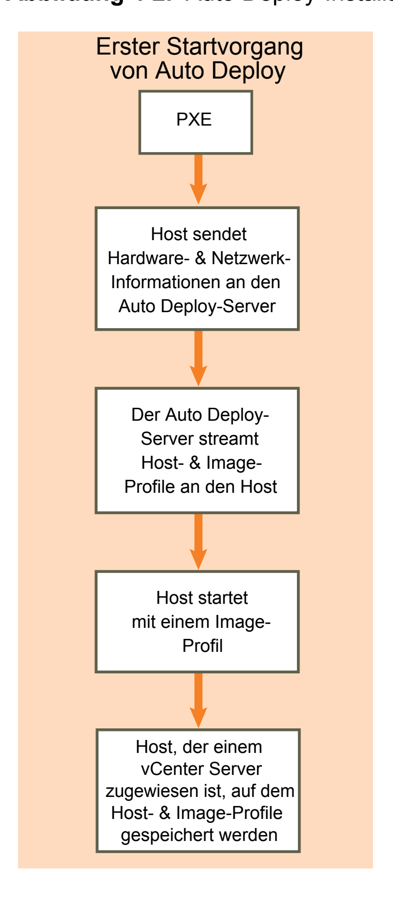
7. (Optional) Wenn das Hostprofil bestimmte Informationen vom Benutzer benötigt, wie z. B. eine statische IP-Adresse, wird der Host in den Wartungsmodus versetzt, wenn der Host zum vCenter Server-System hinzugefügt wird.

   Sie müssen das Hostprofil erneut anwenden und die Host-Anpassung aktualisieren, damit der Host den Wartungsmodus verlassen kann. Wenn Sie die Host-Anpassung aktualisieren, beantworten Sie bei entsprechender Aufforderung alle Fragen.

8. Wenn der Host Teil eines DRS-Clusters ist, werden möglicherweise virtuelle Maschinen von anderen Hosts zum Host migriert werden, nachdem der Host erfolgreich zum vCenter Server-System hinzugefügt wurde.

Siehe „Bereitstellen eines Hosts (erster Start)“, auf Seite 97.

Abbildung 4-2. Auto Deploy-Installation, erster Start



Nachfolgende Startvorgänge ohne Updates

Bei Hosts, die mit Auto Deploy bereitgestellt und durch ein vCenter Server-System verwaltet werden, können nachfolgende Startvorgänge vollautomatisch durchgeführt werden.

1. Der Administrator startet den Host.
2. Beim Starten des Hosts stellt Auto Deploy den Host mit seinem Image- und Hostprofil bereit.
3. Virtuelle Maschinen werden basierend auf den Einstellungen auf dem Host gestartet oder dorthin migriert.
   - Eigenständiger Host. Virtuelle Maschinen werden gemäß den auf dem Host definierten Autostart-Regeln eingeschaltet.
   - DRS-Cluster-Host. Virtuelle Maschinen, die erfolgreich auf andere Hosts migriert wurden, verbleiben dort. Virtuelle Maschinen, für die kein Host über genügend Ressourcen verfügt hat, werden mit dem neu gestarteten Host registriert.

Falls das vCenter Server-System nicht verfügbar ist, kontaktiert der Host Auto Deploy und wird mit einem Image-Profil bereitgestellt. Der Host kontaktiert weiterhin den Auto Deploy-Server, bis Auto Deploy eine erneute Verbindung mit dem vCenter Server-System herstellt.

Auto Deploy kann keine vSphere Distributed Switches einrichten, wenn vCenter Server nicht verfügbar ist, und virtuelle Maschinen werden Hosts nur dann zugewiesen, wenn sie sich in einem HA-Cluster befinden. Erst wenn der Host eine erneute Verbindung mit vCenter Server hergestellt hat und das Hostprofil angewendet wurde, kann der Switch erstellt werden. Da sich der Host im Wartungsmodus befindet, können die virtuellen Maschinen nicht gestartet werden. Siehe „Erneute Bereitstellung von Hosts mit einfachen Neustartvorgängen“, auf Seite 99.

Hosts, die so eingerichtet sind, dass eine Benutzereingabe erforderlich ist, werden in den Wartungsmodus versetzt. Siehe „Aktualisieren Sie die Hostanpassung im vSphere Web Client“, auf Seite 100.

Nachfolgende Startvorgänge mit Updates

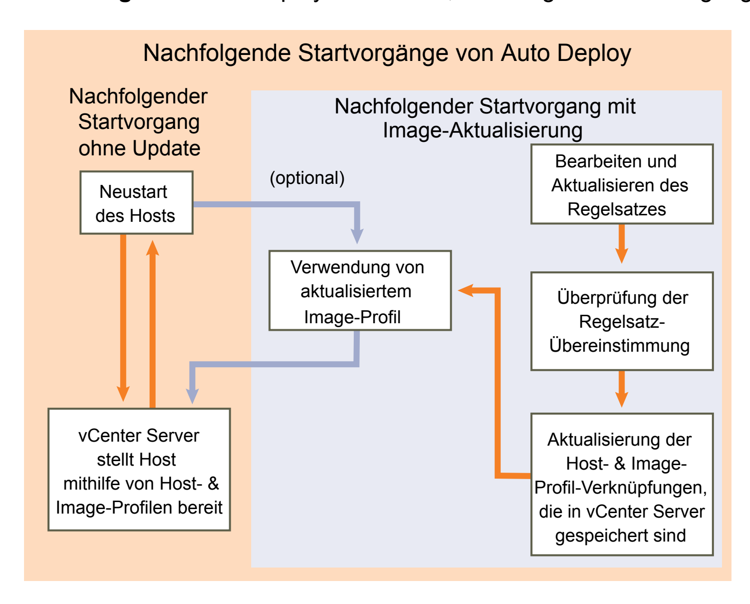
Sie können das Image-Profil, das Hostprofil oder den vCenter Server-Speicherort für Hosts ändern. Der Vorgang umfasst das Ändern der Regeln sowie das Testen und Reparieren der Regelübereinstimmung des Hosts.

1. Der Administrator verwendet das PowerCLI-cmdlet `Copy-DeployRule`, um eine oder mehrere Regeln zu kopieren und zu bearbeiten, und aktualisiert den Regelsatz. Ein Beispiel finden Sie in „Auto Deploy – Schnellstart“, auf Seite 84.
2. Der Administrator führt das cmdlet `Test-DeployRulesetCompliance` aus, um zu prüfen, ob jeder Host die Informationen verwendet, die der aktuelle Regelsatz angibt.
3. Der Host gibt ein PowerCLI-Objekt zurück, das die Übereinstimmungsinformationen einkapselt.
4. Der Administrator führt das cmdlet `Repair-DeployRulesetCompliance` aus, um das Image-Profil, das Hostprofil oder den vCenter Server-Speicherort zu aktualisieren, das bzw. den das vCenter Server-System für jeden Host speichert.
5. Wenn der Host neu gestartet wird, verwendet er das aktualisierte Image-Profil, das aktualisierte Hostprofil oder den aktualisierten vCenter Server-Speicherort für den Host.

   Wenn das Hostprofil so eingerichtet ist, dass es Benutzereingaben benötigt, wird der Host in den Wartungsmodus versetzt. Befolgen Sie die unter „Aktualisieren Sie die Hostanpassung im vSphere Web Client“, auf Seite 100 beschriebenen Schritte.

Siehe „Testen und Reparieren der Regelübereinstimmung“, auf Seite 96.

Abbildung 4-3. Auto Deploy-Installation, Nachfolgende Startvorgänge



Bereitstellung von Systemen mit Distributed Switches

Sie können das Hostprofil eines Auto Deploy-Referenzhosts mit einem Distributed Switch konfigurieren.

Wenn Sie den Distributed Switch konfigurieren, wird die Startkonfigurationsparameter-Richtlinie automatisch auf die Netzwerkparameter eingestellt, die nach einem Neustart zum Herstellen der Hostkonnektivität erforderlich sind.

Wenn Auto Deploy den ESXi-Host mit dem Hostprofil bereitstellt, durchläuft der Host einen aus zwei Schritten bestehenden Prozess.

1 Der Host erstellt einen virtuellen Standard-Switch mit den Eigenschaften, die im Feld für die Startkonfigurationsparameter angegeben sind.

2 Der Host erstellt die VMkernel-NICs. Anhand der VMkernel-NICs kann der Host eine Verbindung zu Auto Deploy und dem vCenter Server-System herstellen.

Wenn der Host zum vCenter Server hinzugefügt wird, entfernt vCenter Server den Standard-Switch und wendet den Distributed Switch erneut auf den Host an.

Hinweis Ändern Sie die Startkonfigurationsparameter nicht, um Probleme mit Ihrem Distributed Switch zu vermeiden.

Überblick über die Auto Deploy-Kurzanleitung und Cmdlets

Um Auto Deploy erfolgreich einzusetzen, müssen Sie sich mit den Aufgaben für das Bereitstellen von Hosts vertraut machen, die Auto Deploy-Komponenten und deren Zusammenspiel verstehen und die PowerCLI-cmdlets kennen.

Auto Deploy – Schnellstart

Zu den ersten Schritten mit Auto Deploy gehören das Verständnis der Funktionsweise von Auto Deploy, die Installation des Auto Deploy-Servers, die Installation von vSphere PowerCLI, die Formulierung von vSphere PowerCLI-Regeln zum Bereitstellen von Hosts sowie das Einschalten der Hosts, damit sie anhand eines angegebenen Image-Profils gestartet werden können. Sie können Anpassungen des Image-Profils, des Hostprofils und des Speicherorts von vCenter Server vornehmen.

Unter „Machbarkeitsnachweis-Setup für Auto Deploy“, auf Seite 135 finden Sie eine schrittweise Übung, die Ihnen dabei hilft, Ihre erste Auto Deploy-Umgebung unter Windows Server 2008 einzurichten.

Sie können diese Schritte befolgen, um Hosts in Ihrer Umgebung mit Auto Deploy bereitzustellen.

1 Installieren Sie vCenter Server und die zugehörigen Komponenten oder stellen Sie vCenter Server bereit.

   Der Auto Deploy-Server ist im Verwaltungsknoten enthalten.

2 Installieren Sie vSphere PowerCLI, das die Cmdlets für Auto Deploy und Image Builder enthält.

   Siehe „Installieren von vSphere PowerCLI und erforderlicher Software“, auf Seite 90 und „Verwendung der Auto Deploy-cmdlets“, auf Seite 90.

3 Suchen Sie das Image-Profil, das die VIBs enthält, die Sie für Ihre Hosts bereitstellen möchten.

   - In den meisten Fällen fügen Sie die Depots mit der erforderlichen Software zu Ihrer vSphere PowerCLI-Sitzung hinzu und wählen anschließend ein Image-Profil aus einem dieser Depots aus.
   - Mit Image Builder-cmdlets können Sie ein benutzerdefiniertes Image-Profil erstellen, um ein vorhandenes Image-Profil zu klonen und die benutzerdefinierten VIBs zum Klon hinzuzufügen. Fügen Sie das benutzerdefinierte Image-Profil zur vSphere PowerCLI-Sitzung hinzu.

   Die Verwendung von Image Builder ist nur dann für die Anpassung erforderlich, wenn Sie VIBs hinzufügen oder entfernen müssen. In den meisten Fällen können Sie das Depot, in dem VMware die Image-Profile hostet, als URL zu Ihrer vSphere PowerCLI-Sitzung hinzufügen.

4 Verwenden Sie das vSphere PowerCLI-Cmdlet `New-DeployRule`, um eine Regel zu erstellen, die das Image-Profil einem Host, mehreren anhand eines Musters angegebenen Hosts oder allen Hosts zuweist.

   ```
   New-DeployRule -Name "testrule" -Item image-profile -AllHosts
   ```

Siehe „Zuweisen eines Image-Profils zu Hosts“, auf Seite 93.

Hinweis Auto Deploy ist für das Bereitstellen von Hosts optimiert, die eine feste MAC-Adresse/IP-Adresse-Zuordnung in DHCP aufweisen (mitunter auch als DHCP-Reservierungen bezeichnet). Wenn Sie statische IP-Adressen verwenden möchten, müssen Sie das Hostprofil so einrichten, dass es eine Hostanpassung anfordert. Siehe „Einrichten von Hostprofilen für statische IP-Adressen im vSphere Web Client“, auf Seite 117.

5 Schalten Sie den Host ein, damit Auto Deploy den Host mit dem angegebenen Image-Profil ausstattet.

6 Richten Sie den von Ihnen bereitgestellten Host als Referenzhost für Ihr Hostprofil ein.

Sie können für den Referenzhost die syslog-Einstellungen, die Firewall-Einstellungen, den Speicher, das Netzwerk usw. angeben. Siehe „Einrichten eines Auto Deploy-Referenzhosts“, auf Seite 110.

7 Erstellen und exportieren Sie ein Hostprofil für den Referenzhost.

Weitere Informationen finden Sie in der Dokumentation *Hostprofile*.

8 Mit dem `Copy-DeployRule`-cmdlet können Sie mehrere Hosts bereitstellen.

Sie können die Regel überarbeiten, sodass nicht nur ein Image-Profil, sondern auch ein Hostprofil und ein Clusterspeicherort zugewiesen werden.

```
Copy-DeployRule -DeployRule "testrule" -ReplaceItem my_host_profile_from_refe-
rence_host,my_target_cluster
               -ReplacePattern  "ipv4=192.XXX.1.10-192.XXX.1.20"
```

my_host_profile_from_reference_host ist der Name des Profils des Referenzhosts, *my_target_cluster* jener des Zielclusters.

9 Schalten Sie die gewünschten Hosts ein.

Wenn die anhand des Musters angegebenen Hosts derzeit nicht von einem vCenter Server-System verwaltet werden, stattet sie Auto Deploy mit dem bereits gespeicherten Image-Profil und dem angegebenen Hostprofil aus und fügt sie zum Zielcluster hinzu.

10 Stellen Sie sicher, dass die von Ihnen ausgestatteten Hosts folgende Anforderungen erfüllen:

- Jeder Host ist mit dem vCenter Server-System verbunden.
- Die Hosts befinden sich nicht im Wartungsmodus.
- Die Hosts weisen keine Übereinstimmungsfehler auf.
- Jeder Host mit einem Hostprofil, das Benutzereingaben benötigt, verfügt über die neuesten Informationen zur Hostanpassung.

Beheben Sie die Hostanpassungs- und -übereinstimmungsprobleme und starten Sie die Hosts neu, bis alle Hosts die Anforderungen erfüllen.

Eine Einführung in den Startprozess, die Unterschiede zwischen dem ersten und den nachfolgenden Startvorgängen und die Verwendung der Hostanpassung finden Sie in „Grundlegendes zu vSphere Auto Deploy“, auf Seite 76.

Auto Deploy PowerCLI-cmdlet - Überblick

Sie geben mithilfe eines Satzes von in VMware PowerCLI enthaltenen PowerCLI-cmdlets die Regeln an, die Image-Profilen bereit und Hostprofile zu Hosts zuweisen.

Wenn Sie PowerCLI noch nicht benutzt haben, lesen Sie die Dokumentation zu PowerCLI und „Verwendung der Auto Deploy-cmdlets“, auf Seite 90. Sie können an der PowerShell-Eingabeaufforderung Hilfe zu jedem Befehl erhalten.

- Allgemeine Hilfe: `Get-Help` *Name_des_cmdlets*

- Detaillierte Hilfe: `Get-Help` *Name_des_cmdlets* `-Detailed`

Hinweis Geben Sie bei der Ausführung von Auto Deploy-cmdlets alle Parameter in der Befehlszeile an, wenn Sie das cmdlet aufrufen. Die Angabe von Parametern im interaktiven Modus wird nicht empfohlen.

Tabelle 4-6. Regel-Engine-PowerCLI-cmdlets

Befehl	Beschreibung
`Get-DeployCommand`	Gibt eine Liste von Auto Deploy-cmdlets zurück.
`New-DeployRule`	Erstellt eine neue Regel mit den angegebenen Elementen und Mustern.
`Set-DeployRule`	Aktualisiert eine vorhandene Regel mit den angegebenen Elementen und Mustern. Sie können keine Regel aktualisieren, die Teil eines Regelsatzes ist.
`Get-DeployRule`	Ruft die Regeln mit den angegebenen Namen ab.
`Copy-DeployRule`	Klont und aktualisiert eine vorhandene Regel.
`Add-DeployRule`	Fügt eine oder mehrere Regeln zum Arbeitsregelsatz und standardmäßig auch zum aktiven Regelsatz hinzu. Verwenden Sie den Parameter `NoActivate`, um eine Regel nur zum Arbeitsregelsatz hinzuzufügen.
`Remove-DeployRule`	Entfernt eine oder mehrere Regeln aus dem Arbeits- und dem aktiven Regelsatz. Führen Sie diesen Befehl mit dem Parameter `-Delete` aus, um die Regel vollständig zu löschen.
`Set-DeployRuleset`	Legt die Liste der Regeln im Arbeitsregelsatz explizit fest.
`Get-DeployRuleset`	Ruft den aktuellen Arbeitsregelsatz oder den derzeit aktiven Regelsatz ab.
`Switch-ActiveDeployRuleset`	Aktiviert einen Regelsatz, sodass alle neuen Anforderungen durch den Regelsatz bewertet werden.
`Get-VMHostMatchingRules`	Ruft Regeln ab, die einem Muster entsprechen. Sie können beispielsweise alle Regeln abrufen, die sich auf einen Host oder auf mehrere Hosts beziehen. Verwenden Sie dieses cmdlet in erster Linie für das Debuggen.
`Test-DeployRulesetCompliance`	Prüft, ob die Elemente, die einem bestimmten Host zugeordnet sind, mit dem aktiven Regelsatz übereinstimmen.
`Repair-DeployRulesetCompliance`	Anhand der Ausgabe von `Test-DeployRulesetCompliance` aktualisiert dieses cmdlet das Image-Profil, das Hostprofil und den Speicherort für jeden Host in der vCenter Server-Bestandsliste. Das cmdlet wendet möglicherweise Image-Profilen bereit und Hostprofile an oder verschiebt Hosts in vorgegebene Ordner oder Cluster auf dem vCenter Server-System.
`Apply-EsxImageProfile`	Ordnet das angegebene Image-Profil dem angegebenen Host zu.
`Get-VMHostImageProfile`	Ruft das Image-Profil ab, das der angegebene Host verwendet. Dieses cmdlet unterscheidet sich von dem `Get-EsxImageProfile`-cmdlet der Image Builder PowerCLI.
`Repair-DeployImageCache`	Verwenden Sie dieses cmdlet nur dann, wenn der Auto Deploy-Image-Cache versehentlich gelöscht wurde.
`Get-VMHostAttributes`	Ruft die Attribute für einen Host ab, die verwendet werden, wenn der Auto Deploy-Server die Regeln auswertet.
`Get-DeployMachineIdentity`	Gibt einen Zeichenfolgenwert zurück, den Auto Deploy verwendet, um einen ESXi-Host in vCenter mit einer physischen Maschine logisch zu verknüpfen.

Tabelle 4-6. Regel-Engine-PowerCLI-cmdlets (Fortsetzung)

Befehl	Beschreibung
`Set-DeployMachineIdentity`	Erstellt eine logische Verknüpfung zwischen einem Hostobjekt in der vCenter Server-Datenbank und einer physischen Maschine. Verwenden Sie dieses cmdlet zum Hinzufügen von Hosts, ohne Regeln anzugeben.
`Get-DeployOption`	Ruft die globalen Auto Deploy-Konfigurationsoptionen ab. Dieses cmdlet unterstützt zurzeit die Option `vlan-id`, die die Standard-VLAN-ID für das ESXi-Verwaltungsnetzwerk eines mit Auto Deploy bereitgestellten Hosts angibt. Auto Deploy verwendet den Wert nur dann, wenn der Host ohne ein Hostprofil gestartet wird.
`Set-DeployOption`	Legt den Wert einer globalen Konfigurationsoption fest. Unterstützt zurzeit die Option `vlan-id`, die die Standard-VLAN-ID für das ESXi-Verwaltungsnetzwerk festlegt.

Vorbereitung für vSphere Auto Deploy

Sie müssen Ihre Umgebung auf die Verwendung von vSphere Auto Deploy vorbereiten. Sie beginnen mit dem Einrichten des Servers und der Vorbereitung der Hardware. Sie müssen die Auto Deploy-Software mit dem vCenter Server-System registrieren, das Sie für die Verwaltung der von Ihnen bereitgestellten Hosts verwenden möchten, und VMware PowerCLI installieren.

- Vorbereiten des Systems und Installieren des Auto Deploy-Servers auf Seite 87

  Bevor Sie einen ESXi-Host mit PXE und vSphere Auto Deploy starten können, müssen Sie die erforderliche Software installieren und die DHCP- und TFTP-Server einrichten, mit denen Auto Deploy interagiert.

- Installieren von vSphere PowerCLI und erforderlicher Software auf Seite 90

  Bevor Sie Auto Deploy-cmdlets zum Erstellen und Ändern der Regeln und Regelsätze, die das Verhalten von Auto Deploy steuern, ausführen, müssen Sie vSphere PowerCLI und alle erforderliche Software installieren. Die Auto Deploy-cmdlets sind im Lieferumfang der vSphere PowerCLI-Installation enthalten.

- Verwendung der Auto Deploy-cmdlets auf Seite 90

  Auto Deploy-Cmdlets werden als Microsoft PowerShell-Cmdlets implementiert und sind in vSphere PowerCLI enthalten. Benutzer von Auto Deploy-Cmdlets haben den Vorteil, alle vSphere PowerCLI-Funktionen nutzen zu können.

- Einrichten der Massenlizenzierung auf Seite 91

  Sie können den vSphere Web Client oder die ESXi Shell dazu verwenden, einzelne Lizenzschlüssel anzugeben, oder Sie können die Massenlizenzierung mithilfe der PowerCLI-cmdlets einrichten. Die Massenlizenzierung kann auf allen ESXi-Hosts eingesetzt werden, ist jedoch besonders nützlich für mit Auto Deploy bereitgestellte Hosts.

Vorbereiten des Systems und Installieren des Auto Deploy-Servers

Bevor Sie einen ESXi-Host mit PXE und vSphere Auto Deploy starten können, müssen Sie die erforderliche Software installieren und die DHCP- und TFTP-Server einrichten, mit denen Auto Deploy interagiert.

Voraussetzungen

- Stellen Sie sicher, dass die Hosts, die Sie mit Auto Deploy bereitstellen möchten, den Anforderungen für ESXi entsprechen. Siehe „Hardwareanforderungen für ESXi“, auf Seite 21.

  Hinweis Sie können keine EFI-Hosts mit Auto Deploy bereitstellen, es sei denn, Sie versetzen die EFI-Systeme in den BIOS-Kompatibilitätsmodus.

- Stellen Sie sicher, dass die ESXi-Hosts über eine Netzwerkverbindung mit vCenter Server verfügen und alle Portanforderungen erfüllt sind. Siehe „Erforderliche Ports für vCenter Server", auf Seite 32.
- Wenn Sie in Ihrer Auto Deploy-Umgebung VLANs verwenden möchten, müssen Sie das End-to-End-Netzwerk ordnungsgemäß einrichten. Wenn der Host per PXE gestartet wird, muss der UNDI-Treiber für das Taggen der Frames mit den richtigen VLAN-IDs konfiguriert werden. Sie müssen diese Konfiguration manuell durchführen, indem Sie im BIOS die entsprechenden Änderungen vornehmen. Außerdem müssen die ESXi-Portgruppen mit den richtigen VLAN-IDs konfiguriert werden. Fragen Sie Ihren Netzwerkadministrator, wie VLAN-IDs in Ihrer Umgebung verwendet werden.
- Stellen Sie sicher, dass der Speicher für das Auto Deploy-Repository ausreicht. Der Auto Deploy-Server verwendet das Repository zum Speichern der erforderlichen Daten, dazu zählen die von Ihnen erstellten Regeln und Regelsätze und die VIBs und Image-Profile, die Sie in Ihren Regeln angeben.

  Es wird empfohlen, 2 GB zuzuweisen, damit Sie ausreichend Speicherplatz für vier Image-Profile und etwas zusätzlichen Speicherplatz in Reserve haben. Für jedes Image-Profil werden ungefähr 350 MB benötigt. Berechnen Sie den Speicherplatzbedarf für das Auto Deploy-Repository anhand der Anzahl der Image-Profilen bereit, die Sie voraussichtlich verwenden werden.
- Verschaffen Sie sich Administratorrechte für den DHCP-Server, der das Netzwerksegment verwaltet, von dem Sie starten möchten. Sie können einen bereits in Ihrer Umgebung vorhandenen DHCP-Server verwenden oder einen DHCP-Server installieren. Ersetzen Sie für Ihr Auto Deploy-Setup den Dateinamen `gpxelinux.0` durch `undionly.kpxe.vmw-hardwired`.
- Sichern Sie Ihr Netzwerk wie bei jeder anderen PXE-basierten Bereitstellungsmethode. Auto Deploy überträgt Daten über SSL, um gelegentliche Störungen und Webspionage zu verhindern Allerdings wird die Authentizität des Clients oder des Auto Deploy-Servers während des Startens per PXE-Startvorgang nicht überprüft.
- Richten Sie einen Remote-Syslog-Server ein. Weitere Informationen zur Konfiguration eines Syslog-Servers finden Sie in der Dokumentation zu *vCenter Server und Hostverwaltung*. Konfigurieren Sie den ersten Host, den Sie zum Verwenden des Remote-Syslog-Servers starten, und wenden Sie das Hostprofil dieses Hosts auf alle anderen Zielhosts an. Sie können optional vSphere Syslog Collector, ein vCenter Server-Dienstprogramm, das eine einheitliche Architektur für die Systemprotokollierung bietet sowie die Netzwerkprotokollierung und das Kombinieren von Protokollen mehrerer Hosts ermöglicht, installieren und verwenden.
- Installieren Sie ESXi Dump Collector und richten Sie Ihren ersten Host so ein, dass alle Core-Dumps auf ESXi Dump Collector verwiesen werden. Wenden Sie anschließend das Hostprofil von diesem Host auf alle anderen Hosts an. Siehe „Konfigurieren des ESXi Dump Collectors mit ESXCLI", auf Seite 112.
- Stellen Sie sicher, dass der Auto Deploy-Server über eine IPv4-Adresse verfügt. Auto Deploy bietet keine End-to-End-Unterstützung für reine IPv6-Umgebungen. IPv6 wird von der PXE-Start-Infrastruktur nicht unterstützt. Nach der Bereitstellung können Sie die Hosts für die Verwendung von IPv6 manuell neu konfigurieren und dem vCenter Server über IPv6 hinzufügen. Beim Neustart eines statusfreien Hosts geht die IPv6-Konfiguration allerdings verloren.

Vorgehensweise

1. Installieren Sie vCenter Server oder stellen Sie vCenter Server Appliance bereit.

   Der Auto Deploy-Server ist im Verwaltungsknoten enthalten.
2. Konfigurieren Sie den Starttyp des Auto Deploy-Diensts.
   a. Melden Sie sich über vSphere Web Client beim vCenter Server-System an.
   b. Klicken Sie auf der Startseite von vSphere Web Client auf **Verwaltung**.

c Klicken Sie unter **Systemkonfiguration** auf **Dienste**.

d Wählen Sie **Auto Deploy**, klicken Sie auf das Menü **Aktionen** und wählen Sie **Starttyp bearbeiten**.

- Unter Windows ist der Auto Deploy-Dienst deaktiviert. Wählen Sie im Fenster Starttyp bearbeiten die Optionen **Manuell** oder **Automatisch**, um Auto Deploy zu aktivieren.

- In vCenter Server Appliance ist der Auto Deploy-Dienst standardmäßig auf **Manuell** gesetzt. Wenn Sie möchten, dass der Auto Deploy-Dienst beim Start des Betriebssystems automatisch gestartet wird, wählen Sie **Automatisch**.

3 Konfigurieren Sie den TFTP-Server.

a Wechseln Sie in einem vSphere Web Client, der mit dem vCenter Server-System verbunden ist, in die Bestandsliste und wählen Sie das vCenter Server-System aus.

b Klicken Sie auf die Registerkarte **Verwalten**, wählen Sie **Einstellungen** und klicken Sie auf **Auto Deploy**.

c Klicken Sie auf **TFTP Boot Zip herunterladen**, um die TFTP-Konfigurationsdatei herunterzuladen, und entpacken Sie die Datei in dem Verzeichnis, in dem der TFTP-Server Dateien speichert.

4 Richten Sie Ihren DHCP-Server so ein, dass er auf den TFTP-Server verweist, auf dem sich die TFTP-ZIP-Datei befindet.

a Geben Sie in DHCP-Option 66 (oft als „next-server“ bezeichnet) die IP-Adresse des TFTP-Servers ein.

b Geben Sie den Namen der Startdatei (`undionly.kpxe.vmw-hardwired`) in DHCP-Option 67 (oft als `boot-filename` bezeichnet) ein.

5 Richten Sie jeden mit Auto Deploy bereitzustellenden Host für das Starten über das Netzwerk oder per PXE-Startvorgang gemäß den Anweisungen des Anbieters ein.

6 Suchen Sie das Image-Profil, das Sie verwenden möchten, und das Depot, in dem es sich befindet.

In den meisten Fällen können Sie auf ein Image-Profil verweisen, das VMware in einem öffentlichen Depot zur Verfügung stellt. Wenn Sie benutzerdefinierte VIBs in das Basis-Image einbinden möchten, erstellen Sie mit vSphere ESXi Image Builder ein Image-Profil und verwenden Sie dieses.

7 Schreiben Sie eine Regel, die den Hosts ein Image-Profil zuweist.

8 (Optional) Wenn Sie Ihre Umgebung für den Einsatz des Fingerabdruckmodus einrichten, können Sie Ihre eigene Zertifizierungsstelle (CA) verwenden, indem Sie das OpenSSL-Zertifikat `rbd-ca.crt` und den privaten OpenSSL-Schlüssel `rbd-ca.key` durch ein eigenes Zertifikat und eine eigene Schlüsseldatei ersetzen.

- Unter Windows befinden sich die Dateien im Unterordner „SSL“ des Auto Deploy-Installationsverzeichnisses. Unter Windows 7 ist z. B. der Standardordner `C:\ProgramData\VMware\VMware vSphere Auto Deploy\ssl`.

- Auf der vCenter Server Appliance befinden sich die Dateien im Verzeichnis `/etc/vmware-rbd/ssl/`.

Standardmäßig verwenden vCenter Server 6.0 und höher die vSphere-Zertifizierungsstelle.

Wenn Sie einen Host einschalten, der für Auto Deploy eingerichtet ist, kontaktiert der Host den DHCP-Server und wird an den Auto Deploy-Server verwiesen, der den Host mit dem Image-Profil bereitstellt, das im aktiven Regelsatz angegeben ist.

Weiter

- Installieren Sie vSphere PowerCLI. Siehe „Installieren von vSphere PowerCLI und erforderlicher Software“, auf Seite 90.

- Verwenden Sie die vSphere PowerCLI-Cmdlets zum Definieren einer Regel, die dem Host ein Image-Profil und optional ein Hostprofil zuweist.

- (Optional) Konfigurieren Sie den ersten Host, den Sie bereitstellen, als Referenzhost. Verwenden Sie die Speicher- und Netzwerkeinstellungen sowie weitere Einstellungen, die Sie auf Ihren Zielhosts freigeben möchten. Erstellen Sie ein Hostprofil für den Referenzhost und schreiben Sie eine Regel, die den Zielhosts sowohl das bereits getestete Image-Profil als auch das Hostprofil zuweist.
- Wenn Auto Deploy die vorhandenen Partitionen überschreiben soll, richten Sie einen Referenzhost für die Durchführung der automatischen Partitionierung ein und wenden Sie das Hostprofil des Referenzhosts auf andere Hosts an. Siehe „Berücksichtigen und Implementieren Ihrer Partitionierungsstrategie“, auf Seite 117.
- Wenn Sie hostspezifische Informationen konfigurieren müssen, richten Sie das Hostprofil des Referenzhosts so ein, dass Benutzer zur Eingabe von Informationen aufgefordert werden. Siehe „Hostanpassung im vSphere Web Client“, auf Seite 118.

Installieren von vSphere PowerCLI und erforderlicher Software

Bevor Sie Auto Deploy-cmdlets zum Erstellen und Ändern der Regeln und Regelsätze, die das Verhalten von Auto Deploy steuern, ausführen, müssen Sie vSphere PowerCLI und alle erforderliche Software installieren. Die Auto Deploy-cmdlets sind im Lieferumfang der vSphere PowerCLI-Installation enthalten.

Sie installieren vSphere PowerCLI und die erforderliche Software auf einem Microsoft Windows-System. Weitere Informationen zur Installation der Microsoft-Software finden Sie auf der Microsoft-Website. Das *Benutzerhandbuch für vSphere PowerCLI* enthält detaillierte Anweisungen zum Installieren von vSphere PowerCLI.

Voraussetzungen

- Stellen Sie sicher, dass Microsoft .NET 4.5 SP2 installiert ist, oder installieren Sie es von der Microsoft-Website aus gemäß den Anweisungen auf dieser Website.
- Stellen Sie sicher, dass Windows PowerShell 3.0 installiert ist, oder installieren Sie es von der Microsoft-Website aus gemäß den Anweisungen auf dieser Website.

Vorgehensweise

◆ Installieren Sie vSphere PowerCLI, in der die Auto Deploy-cmdlets enthalten sind.

Weiter

Lesen Sie „Verwendung der Auto Deploy-cmdlets“, auf Seite 90 durch. Wenn Sie vSphere PowerCLI noch nicht benutzt haben, lesen Sie die Dokumentation zu vSphere PowerCLI.

Verwenden Sie Auto Deploy- sowie andere vSphere PowerCLI- und PowerShell-cmdlets zum Verwalten der Auto Deploy-Regeln und -Regelsätze. Sie können mithilfe von `Get-Help`*`Name_des_cmdlets`* Hilfe aufrufen.

Verwendung der Auto Deploy-cmdlets

Auto Deploy-Cmdlets werden als Microsoft PowerShell-Cmdlets implementiert und sind in vSphere PowerCLI enthalten. Benutzer von Auto Deploy-Cmdlets haben den Vorteil, alle vSphere PowerCLI-Funktionen nutzen zu können.

Erfahrene PowerShell-Benutzer können Auto Deploy-cmdlets genau wie andere PowerShell-cmdlets verwenden. Wenn Sie PowerShell und vSphere PowerCLI erst seit Kurzem verwenden, sind möglicherweise die folgenden Tipps hilfreich.

Sie können Cmdlets, Parameter und Parameterwerte in die vSphere PowerCLI-Shell eingeben.

- Sie erhalten Hilfe zu jedem cmdlet , indem Sie `Get-Help` *`Name_des_cmdlets`* ausführen.
- Beachten Sie, dass bei PowerShell die Groß-/Kleinschreibung nicht beachtet wird.
- Verwenden Sie die Tabulatortaste zum Vervollständigen der cmdlet- und Parameternamen.

- Formatieren Sie die Ausgabe von Variablen und Cmdlets mit `Format-List` oder `Format-Table` bzw. deren Kurzformen `flfl` oder `ft`. Um weitere Informationen zu erhalten, führen Sie das Cmdlet `Get-Help Format-List` aus.

Übergeben von Parametern per Name

Sie können in den meisten Fällen Parameter per Name übergeben und Parameterwerte, die Leer- oder Sonderzeichen enthalten, in doppelte Anführungszeichen einschließen.

```
Copy-DeployRule -DeployRule testrule -ReplaceItem MyNewProfile
```

Bei den meisten Beispielen in der Dokumentation zu *Installations- und Einrichtungshandbuch für vSphere* werden Parameter nach Namen übergeben.

Übergeben von Parametern als Objekte

Für Scripting und Automatisierung können Sie Parameter als Objekte übergeben. Das Übergeben von Parametern als Objekte ist sowohl nützlich bei cmdlets, die mehrere Objekte zurückgeben, als auch bei cmdlets, die ein einzelnes Objekt zurückgeben. Beachten Sie das folgende Beispiel.

1 Binden Sie das Objekt, das die Regelsatz-Übereinstimmungsinformationen für einen Host einkapselt, an eine Variable.

   ```
   $tr = Test-DeployRuleSetCompliance MyEsxi42
   ```

2 Zeigen Sie die Eigenschaft `itemlist` des Objekts an, um den Unterschied zu sehen zwischen dem, was sich im Regelsatz befindet, und dem, was der Host aktuell verwendet.

   ```
   $tr.itemlist
   ```

3 Standardisieren Sie den Host, sodass er den überarbeiteten Regelsatz nutzt. Verwenden Sie dazu mit der Variablen das Cmdlet `Repair-DeployRuleSetCompliance`.

   ```
   Repair-DeployRuleSetCompliance $tr
   ```

Im Beispiel wird der Host standardisiert, wenn Sie ihn das nächste Mal starten.

Einrichten der Massenlizenzierung

Sie können den vSphere Web Client oder die ESXi Shell dazu verwenden, einzelne Lizenzschlüssel anzugeben, oder Sie können die Massenlizenzierung mithilfe der PowerCLI-cmdlets einrichten. Die Massenlizenzierung kann auf allen ESXi-Hosts eingesetzt werden, ist jedoch besonders nützlich für mit Auto Deploy bereitgestellte Hosts.

Im folgenden Beispiel werden allen Hosts in einem Datencenter Lizenzen zugewiesen. Sie können auch Lizenzen mit Hosts und Clustern verknüpfen.

Das folgende Beispiel richtet sich an fortgeschrittene PowerCLI-Benutzer, die mit der Verwendung von PowerShell-Variablen vertraut sind.

Voraussetzungen

Installieren Sie PowerCLI. Weitere Informationen hierzu finden Sie unter „Installieren von vSphere PowerCLI und erforderlicher Software“, auf Seite 90.

Die Zuweisung von Lizenzschlüsseln über den vSphere Web Client und die Zuweisung von Lizenzen mithilfe von PowerCLI-cmdlets funktionieren unterschiedlich.

Zuweisen von Lizenzschlüsseln mit dem vSphere Web Client
Sie können einem Host Lizenzschlüssel zuweisen, wenn Sie den Host zum vCenter Server-System hinzufügen oder wenn der Host von einem vCenter Server-System verwaltet wird.

Zuweisen von Lizenzschlüsseln mit LicenseDataManager PowerCLI
Sie können mehrere Lizenzschlüssel angeben, die zu mehreren Hosts hinzugefügt werden sollen. Die Lizenzschlüssel werden in die vCenter Server-Datenbank aufgenommen. Jedes Mal, wenn ein Host zum vCenter Server-System hinzugefügt wird oder sich erneut mit dem vCenter Server-System verbindet, wird dem Host ein Lizenzschlüssel zugewiesen. Ein Lizenzschlüssel, der über die PowerCLI zugewiesen wird, wird als Standardlizenzschlüssel angesehen. Wenn ein nicht lizenzierter Host hinzugefügt oder erneut verbunden wird, wird ihm der Standardlizenzschlüssel zugewiesen. Wenn ein Host bereits lizenziert ist, behält er seinen Lizenzschlüssel bei.

Vorgehensweise

1 Stellen Sie eine Verbindung mit dem vCenter Server-System her, das Sie verwenden möchten, und binden Sie den zugewiesenen Lizenz-Manager an eine Variable.

```
Connect-VIServer -Server 192.XXX.X.XX -User username -Password password
$licenseDataManager = Get-LicenseDataManager
```

2 Führen Sie ein cmdlet aus, das das Datencenter abruft, in dem sich die Hosts befinden, für die Sie die Massenlizenzierungsfunktion verwenden möchten.

```
$hostContainer = Get-Datacenter -Name Datacenter-X
```

Sie können auch ein cmdlet ausführen, das einen Cluster abruft, wobei die Massenlizenzierung für alle darin enthaltenen Hosts durchgeführt werden soll, oder das einen Ordner abruft, wobei die Massenlizenzierung für alle Hosts dieses Ordners durchgeführt werden soll.

3 Erstellen Sie ein neues `LicenseData`-Objekt und ein `LicenseKeyEntry`-Objekt mit zugewiesener Typ-ID und Lizenzschlüssel.

```
$licenseData = New-Object VMware.VimAutomation.License.Types.LicenseData
$licenseKeyEntry = New-Object Vmware.VimAutomation.License.Types.LicenseKeyEntry
$licenseKeyEntry.TypeId = "vmware-vsphere”
$licenseKeyEntry.LicenseKey = "XXXXX-XXXXX-XXXXX-XXXXX-XXXXX"
```

4 Verknüpfen Sie das `LicenseKeys`-Attribut des `LicenseData`-Objekts, das Sie in Schritt 3 erstellt haben, mit dem `LicenseKeyEntry`-Objekt.

```
$licenseData.LicenseKeys += $licenseKeyEntry
```

5 Aktualisieren Sie die Lizenzdaten für das Datencenter mit dem `LicenseData`-Objekt und stellen Sie sicher, dass die Lizenz dem Host-Container zugewiesen ist.

```
$licenseDataManager.UpdateAssociatedLicenseData($hostContainer.Uid, $licenseData)
$licenseDataManager.QueryAssociatedLicenseData($hostContainer.Uid)
```

6 Stellen Sie einen oder mehrere Hosts mit Auto Deploy bereit und weisen Sie sie dem Datencenter oder dem Cluster zu, denen Sie die Lizenzdaten zugewiesen haben.

7 Mit dem vSphere Web Client können Sie sicherstellen, dass der Host erfolgreich der Standardlizenz `XXXXX-XXXXX-XXXXX-XXXXX-XXXXX` zugewiesen wurde.

Alle Hosts, die Sie dem Datencenter zugewiesen haben, werden nun automatisch lizenziert.

Verwalten von Auto Deploy mithilfe von PowerCLI-cmdlets

Mithilfe von Auto Deploy PowerCLI-cmdlets können Sie Regeln erstellen, die Hosts mit Image-Profilen, Hostprofilen und einem Speicherort auf dem vCenter Server-Ziel verknüpfen. Sie können Hosts auch aktualisieren, indem Sie die Einhaltung der Regeln testen und alle Übereinstimmungsprobleme beheben.

Zuweisen eines Image-Profils zu Hosts

Bevor Sie einen Host bereitstellen können, müssen Sie Regeln erstellen, die jedem Host, den Sie unter Verwendung von Auto Deploy bereitstellen möchten, ein Image-Profil zuweisen.

Auto Deploy-Erweiterbarkeitsregeln erzwingen, dass VIBs auf CommunitySupported-Ebene nur Dateien von bestimmten, vordefinierten Speicherorten wie dem ESXCLI-Plug-In-Pfad, dem Jumpstart-Plug-In-Pfad usw. enthalten dürfen. Wenn Sie ein VIB an einem anderen Speicherort einem Image-Profil hinzufügen, wird eine Warnung ausgegeben. Sie können die Warnung mit der Option `force` außer Kraft setzen.

Wenn Sie das Cmdlet `New-DeployRule` für ein Image-Profil aufrufen, das VIBs auf der CommunitySupported-Ebene enthält, welche die Regel verletzen, legen Sie `$DeployNoSignatureCheck = $true` fest, bevor Sie das Image-Profil hinzufügen. Mit dieser Einstellung ignoriert das System die Validierung der Signatur und führt die Erweiterungsregelprüfung nicht durch.

Hinweis Image-Profile, die VIBs auf CommunitySupported-Ebene enthalten, werden in Produktionssystemen nicht unterstützt.

Voraussetzungen

- Installieren Sie VMware PowerCLI und alle erforderliche Software.
- Falls Probleme beim Ausführen der PowerCLI-cmdlets auftreten, sollten Sie in Betracht ziehen, die Ausführungsrichtlinie zu ändern. Weitere Informationen hierzu finden Sie unter „Verwendung der Auto Deploy-cmdlets“, auf Seite 90.

Vorgehensweise

1. Führen Sie das `Connect-VIServer`-PowerCLI-cmdlet aus, um eine Verbindung zum vCenter Server-System herzustellen, mit dem Auto Deploy registriert ist.

   `Connect-VIServer 192.XXX.X.XX`

   Das cmdlet gibt möglicherweise eine Serverzertifikatswarnung zurück. Stellen Sie in einer Produktionsumgebung sicher, dass keine Serverzertifikatswarnungen ausgegeben werden. In einer Entwicklungsumgebung können Sie die Warnung ignorieren.

2. Legen Sie den Speicherort eines öffentlichen Software-Depots fest oder definieren Sie mithilfe der Image Builder PowerCLI ein eigenes Image-Profil.

3. Führen Sie `Add-EsxSoftwareDepot` aus, um das Software-Depot mit dem Image-Profil zur PowerCLI-Sitzung hinzuzufügen.

Depottyp	Cmdlet
Remote-Depot	Führen Sie **`Add-EsxSoftwareDepot`** ***`URL_des_Depots`*** aus.
ZIP-Datei	a Laden Sie die ZIP-Datei auf einen lokalen Dateipfad herunter. b Führen Sie **`Add-EsxSoftwareDepot C:\`*`Dateipfad`*`\`*`Mein_Offline-Depot`*`.zip`** aus.

4 Suchen Sie im Depot nach dem Image-Profil, das Sie verwenden möchten, indem Sie das cmdlet `Get-EsxImageProfile` ausführen.

   Standardmäßig enthält das ESXi-Depot ein Basis-Image-Profil, das VMware Tools und die Zeichenfolge `standard` in seinem Namen enthält, sowie ein Basis-Image-Profil, das VMware Tools nicht enthält.

5 Definieren Sie eine Regel, bei der Hosts mit bestimmten Attributen, z. B. einem Bereich von IP-Adressen, dem Image-Profil zugewiesen werden.

   ```
   New-DeployRule -Name "Testregel" -Item "Mein Profil25" -Pattern "vendor=Acme,Zven",
   "ipv4=192.XXX.1.10-192.XXX.1.20"
   ```

   Doppelte Anführungszeichen sind erforderlich, wenn ein Name Leerzeichen enthält, anderenfalls sind sie optional. Geben Sie anstatt eines Musters `-AllHosts` an, um das Element für alle Hosts zu übernehmen.

   Das cmdlet erstellt eine Regel namens `Testregel`. Die Regel weist das Image-Profil namens „Mein Profil25" allen Hosts mit dem Anbieter Acme oder Zven und einer IP-Adresse im angegebenen Bereich zu.

6 Fügen Sie die Regel dem Regelsatz hinzu.

   ```
   Add-DeployRule Testregel
   ```

   Standardmäßig wird die Regel dem Arbeits- und dem aktiven Regelsatz hinzugefügt. Wenn Sie den Parameter `NoActivate` angeben, wird der Arbeitsregelsatz nicht der aktive Regelsatz.

Wenn der Host von iPXE gestartet wird, meldet er Attribute der Maschine an die Konsole. Verwenden Sie das gleiche Format für die Attribute, wenn Sie Bereitstellungsregeln erstellen.

```
******************************************************************
* Booting through VMware AutoDeploy...
*
* Machine attributes:
* . asset=No Asset Tag
* . domain=vmware.com
* . hostname=myhost.mycompany.com
* . ipv4=XX.XX.XXX.XXX
* . mac=XX:Xa:Xb:Xc:Xx:XX
* . model=MyVendorModel
* . oemstring=Product ID: XXXXXX-XXX
* . serial=XX XX XX XX XX XX...
* . uuid=XXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXX
* . vendor=MyVendor
******************************************************************
```

Weiter

- Bei Hosts, die bereits mit Auto Deploy bereitgestellt wurden, führen Sie die Übereinstimmungstests und die Reparaturvorgänge durch, um Sie mit dem neuen Image-Profil zu versehen. Weitere Informationen hierzu finden Sie unter „Testen und Reparieren der Regelübereinstimmung", auf Seite 96.
- Schalten Sie nicht bereitgestellte Hosts ein, um sie mit dem neuen Image-Profil bereitzustellen.

Erstellen einer Regel und Zuweisen eines Hostprofils zu Hosts

Auto Deploy kann einem oder mehreren Hosts ein Hostprofil zuweisen. Das Hostprofil enthält möglicherweise Informationen über die Speicherkonfiguration, die Netzwerkkonfiguration oder andere Hostmerkmale. Wenn Sie einen Host zum Cluster hinzufügen, wird das Hostprofil des Clusters verwendet.

In vielen Fällen weisen Sie einem Cluster einen Host zu, anstatt explizit ein Hostprofil anzugeben. Der Host verwendet das Hostprofil des Clusters.

Voraussetzungen

- Installieren Sie vSphere PowerCLI und alle erforderlichen Softwareprodukte. Siehe „Installieren von vSphere PowerCLI und erforderlicher Software", auf Seite 90.
- Exportieren Sie das Hostprofil, das Sie verwenden möchten.

Vorgehensweise

1 Führen Sie das `Connect-VIServer`-Cmdlet vSphere PowerCLI aus, um eine Verbindung mit dem vCenter Server-System herzustellen, bei dem Auto Deploy registriert ist.

```
Connect-VIServer 192.XXX.X.XX
```

Das cmdlet gibt möglicherweise eine Serverzertifikatswarnung zurück. Stellen Sie in einer Produktionsumgebung sicher, dass keine Serverzertifikatswarnungen ausgegeben werden. In einer Entwicklungsumgebung können Sie die Warnung ignorieren.

2 Verwenden Sie den vSphere Web Client, um einen Host mit den von Ihnen gewünschten Einstellungen einzurichten und ein Hostprofil dieses Hosts zu erstellen.

3 Sie können den Namen des Hostprofils herausfinden, indem Sie das vSphere PowerCLI-Cmdlet `Get-VMhostProfile` unter Angabe des ESXi-Hosts ausführen, von dem Sie ein Hostprofil erstellen.

4 Definieren Sie an der vSphere PowerCLI-Eingabeaufforderung eine Regel, in der Hosts mit bestimmten Attributen, z. B. einem Bereich von IP-Adressen, dem Hostprofil zugewiesen werden.

```
New-DeployRule -Name "testrule2" -Item my_host_profile -Pattern "vendor=Acme,Zven",
"ipv4=192.XXX.1.10-192.XXX.1.20"
```

Das angegebene Element wird allen Hosts mit den angegebenen Attributen zugewiesen. In diesem Beispiel wird eine Regel namens „Testregel2" angegeben. Die Regel weist das angegebene Hostprofil *my_host_profile* allen Hosts zu, die eine IP-Adresse innerhalb des angegebenen Bereichs und den Anbieter Acme oder Zven aufweisen.

5 Fügen Sie die Regel dem Regelsatz hinzu.

```
Add-DeployRule testrule2
```

Standardmäßig wird der Arbeitsregelsatz zum aktiven Regelsatz und alle Änderungen am Regelsatz werden aktiv, wenn Sie eine Regel hinzufügen. Wenn Sie den Parameter `NoActivate` angeben, wird der Arbeitsregelsatz nicht der aktive Regelsatz.

Weiter

- Weisen Sie dem neuen Host einen bereits mithilfe von Auto Deploy ausgestatteten Host zu, indem Sie Übereinstimmungstests und Reparaturvorgänge auf diesen Hosts durchführen. Weitere Informationen finden Sie unter „Testen und Reparieren der Regelübereinstimmung", auf Seite 96.
- Schalten Sie noch nicht ausgestattete Hosts ein, um sie mit dem Hostprofil auszustatten.

Schreiben einer Regel und Zuweisen eines Hosts zu einem Ordner oder Cluster

Auto Deploy kann einem Ordner oder Cluster einen Host zuweisen. Wenn der Host gestartet wird, fügt ihn Auto Deploy am angegebenen Speicherort auf dem vCenter Server hinzu. Einem Cluster zugewiesene Hosts übernehmen das Hostprofil des Clusters.

Voraussetzungen

- Installieren Sie vSphere PowerCLI und alle erforderliche Software.
- Stellen Sie sicher, dass sich der Ordner, den Sie auswählen, in einem Datencenter oder einem Cluster befindet. Sie können den Host keinem Standalone-Ordner der obersten Ebene zuweisen.

Vorgehensweise

1 Führen Sie das `Connect-VIServer` vSphere PowerCLI-cmdlet aus, um eine Verbindung zum vCenter Server-System herzustellen, mit dem Auto Deploy registriert ist.

```
Connect-VIServer 192.XXX.X.XX
```

Das cmdlet gibt möglicherweise eine Serverzertifikatswarnung zurück. Stellen Sie in einer Produktionsumgebung sicher, dass keine Serverzertifikatswarnungen angezeigt werden. In einer Entwicklungsumgebung können Sie die Warnung ignorieren.

2 Definieren Sie eine Regel, bei der Hosts mit bestimmten Attributen, z. B. einem Bereich von IP-Adressen, einem Ordner oder Cluster zugewiesen werden.

```
New-DeployRule -Name testrule3 -Item "my folder"    -Pattern "vendor=Acme,Zven",
"ipv4=192.XXX.1.10-192.XXX.1.20"
```

In diesem Beispiel wird der Ordnername übergeben. Sie können stattdessen ein Ordner-, Cluster- oder Datencenterobjekt übergeben, das Sie mithilfe des cmdlets `Get-Folder`, `Get-Cluster` bzw. `Get-Datacenter` abrufen.

3 Fügen Sie die Regel dem Regelsatz hinzu.

```
Add-DeployRule testrule3
```

Standardmäßig wird der Arbeitsregelsatz zum aktiven Regelsatz und alle Änderungen am Regelsatz werden aktiv, wenn Sie eine Regel hinzufügen. Wenn Sie den Parameter `NoActivate` angeben, wird der Arbeitsregelsatz nicht der aktive Regelsatz.

Weiter

- Weisen Sie einen Host, der bereits mit Auto Deploy bereitgestellt wurde, der neuen Ordner- oder Clusterposition zu, indem Sie einen Vorgang zum Testen und Reparieren von Übereinstimmungen durchführen. Siehe „Testen und Reparieren der Regelübereinstimmung“, auf Seite 96.
- Schalten Sie nicht bereitgestellte Hosts ein, um sie dem angegebenen vCenter Server-Speicherort hinzuzufügen.

Testen und Reparieren der Regelübereinstimmung

Wenn Sie eine Regel zum Auto Deploy-Regelsatz hinzufügen oder Änderungen an einer oder mehreren Regeln vornehmen, werden die Hosts nicht automatisch aktualisiert. Auto Deploy übernimmt die neuen Regeln nur dann, wenn Sie deren Regelübereinstimmung testen und eine Standardisierung durchführen.

Voraussetzungen

- Installieren Sie vSphere PowerCLI und alle erforderlichen Softwareprodukte.
- Vergewissern Sie sich, dass Ihre Infrastruktur einen oder mehrere ESXi-Hosts enthält, die mit Auto Deploy bereitgestellt wurden, und dass der Host, auf dem vSphere PowerCLI installiert ist, auf diese ESXi-Hosts zugreifen kann.

Vorgehensweise

1 Verwenden Sie vSphere PowerCLI, um zu überprüfen, welche Auto Deploy-Regeln derzeit verfügbar sind.

```
Get-DeployRule
```

Das System gibt die Regeln und die zugeordneten Elemente und Muster zurück.

2 Nehmen Sie an einer der verfügbaren Regeln eine Änderung vor.

   Ändern Sie beispielsweise das Image-Profil und den Namen der Regel.

   ```
   Copy-DeployRule -DeployRule testrule -ReplaceItem MyNewProfile
   ```

   Sie können keine Regel bearbeiten, die bereits zu einem Regelsatz hinzugefügt wurde. Kopieren Sie stattdessen die Regel und ersetzen Sie das Element oder Muster, das Sie ändern möchten.

3 Vergewissern Sie sich, dass Sie auf den Host zugreifen können, dessen Regelsatzübereinstimmung Sie testen möchten.

   ```
   Get-VMHost -Name MyEsxi42
   ```

4 Führen Sie das cmdlet aus, das die Regelsatzübereinstimmung für den Host testet, und binden Sie den Rückgabewert zur späteren Verwendung an eine Variable.

   ```
   $tr = Test-DeployRuleSetCompliance MyEsxi42
   ```

5 Untersuchen Sie die Unterschiede zwischen dem Inhalt des Regelsatzes und der Konfiguration des Hosts.

   ```
   $tr.itemlist
   ```

   Das System gibt eine Tabelle der aktuellen und der erwarteten Elemente zurück.

   ```
   CurrentItem                          ExpectedItem
   -----------                          ------------
   My Profile 25                        MyProfileUpdate
   ```

6 Standardisieren Sie den Host, sodass er beim nächsten Neustart den überarbeiteten Regelsatz verwendet.

   ```
   Repair-DeployRuleSetCompliance $tr
   ```

Weiter

Wenn mit der von Ihnen geänderten Regel der Speicherort für die Bestandsliste angegeben wurde, werden die Änderungen wirksam, wenn Sie die Übereinstimmung reparieren. Starten Sie bei allen anderen Änderungen Ihren Host neu, um die neue Regel mithilfe von Auto Deploy anzuwenden und eine Übereinstimmung zwischen dem Regelsatz und dem Host zu erzielen.

Bereitstellen von ESXi-Systemen mit vSphere Auto Deploy

vSphere Auto Deploy kann Hunderte von physischen Hosts mit ESXi-Software bereitstellen. Sie können Hosts bereitstellen, auf denen zuvor keine ESXi-Software ausgeführt wurde (erster Start), Hosts neu starten oder Hosts mit einem anderen Image-Profil, Hostprofil oder Ordner- bzw. Clusterspeicherort neu bereitstellen.

Der Auto Deploy-Prozess unterscheidet sich je nach dem Zustand des Hosts und den Änderungen, die Sie vornehmen möchten.

Bereitstellen eines Hosts (erster Start)

Die Bereitstellung eines Hosts, der noch nie bereitgestellt wurde, mit Auto Deploy (erster Start) unterscheidet sich von nachfolgenden Startprozessen. Sie müssen den Host vorbereiten und alle sonstigen Voraussetzungen erfüllen, bevor Sie den Host bereitstellen können. Sie können optional mit Image Builder PowerCLI-cmdlets ein benutzerdefiniertes Image-Profil definieren.

Voraussetzungen

- Stellen Sie sicher, dass Ihr Host die Hardwareanforderungen für ESXi-Hosts erfüllt.

  Weitere Informationen hierzu finden Sie unter „Hardwareanforderungen für ESXi“, auf Seite 21.

- Bereiten Sie das System für vSphere Auto Deploy vor (siehe „Vorbereitung für vSphere Auto Deploy“, auf Seite 87).
- Erstellen Sie Regeln, die dem Host ein Image-Profil zuweisen, und weisen Sie dem Host optional ein Hostprofil und einen Speicherort für vCenter Server zu. Weitere Informationen hierzu finden Sie unter „Verwalten von Auto Deploy mithilfe von PowerCLI-cmdlets“, auf Seite 93.

  Nach Abschluss der Einrichtung sind der Auto Deploy-Server und PowerCLI installiert, das DHCP-Setup ist abgeschlossen und die Regeln für den Host, den Sie bereitstellen möchten, befinden sich im aktiven Regelsatz.

Vorgehensweise

1. Schalten Sie den Host ein.

   Der Host kontaktiert den DHCP-Server und lädt iPXE vom Speicherort herunter, auf den der Server verweist. Dann stellt der Auto Deploy-Server den Host mit dem von der Regel-Engine angegebenen Image bereit. Möglicherweise wendet der Auto Deploy-Server ein Hostprofil auf den Host an, sofern im Regelsatz ein Hostprofil angegeben ist. Schließlich fügt Auto Deploy den Host zum vCenter Server-System hinzu, das in der Regel-Engine angegeben ist.
2. (Optional) Wenn Auto Deploy ein Hostprofil anwendet, das Benutzereingaben, wie z. B. eine IP-Adresse, erfordert, wird der Host in den Wartungsmodus versetzt. Wenden Sie im vSphere Web Client das Hostprofil erneut an und reagieren Sie auf die Eingabeaufforderungen.

Nach dem ersten Startvorgang wird der Host ausgeführt und von einem vCenter Server-System verwaltet. vCenter Server speichert das Image-Profil des Hosts, das Hostprofil und Speicherortinformationen.

Sie können den Host jetzt nach Bedarf starten. Nach jedem Start wird der Host vom vCenter Server-System neu bereitgestellt.

Weiter

Stellen Sie Hosts nach Bedarf neu bereit. Weitere Informationen hierzu finden Sie unter „Erneute Bereitstellung von Hosts“, auf Seite 98.

Wenn Sie das Image-Profil, das Hostprofil oder den Speicherort des Hosts ändern möchten, aktualisieren Sie die Regeln und führen Sie den Vorgang zum Testen und Reparieren der Regelübereinstimmung durch. Weitere Informationen hierzu finden Sie unter „Testen und Reparieren der Regelübereinstimmung“, auf Seite 96.

Erneute Bereitstellung von Hosts

vSphere Auto Deploy unterstützt mehrere Optionen zur erneuten Bereitstellung. Sie können einen einfachen Neustart durchführen oder mit einem anderen Image- oder Hostprofil erneut bereitstellen.

Bei einem ersten Start mithilfe von Auto Deploy ist es erforderlich, dass Sie Ihre Umgebung einrichten und Regeln zum Regelsatz hinzufügen. Weitere Informationen hierzu finden Sie unter „Vorbereitung für vSphere Auto Deploy“, auf Seite 87.

Die folgenden Vorgänge zur erneuten Bereitstellung sind vorhanden.

- Einfacher Neustart.
- Neustart von Hosts, für die der Benutzer Fragen während des Startvorgangs beantwortet hat.
- Erneute Bereitstellung mit einem anderen Image-Profil.
- Erneute Bereitstellung mit einem anderen Hostprofil.

Erneute Bereitstellung von Hosts mit einfachen Neustartvorgängen

Für einen einfachen Neustart eines Hosts, der mit Auto Deploy bereitgestellt wird, müssen nur weiterhin alle Voraussetzungen erfüllt sein. Der Prozess verwendet das zuvor zugewiesene Image-Profil, das Hostprofil und den Speicherort von vCenter Server.

Die Einrichtung umfasst die DHCP-Server-Einrichtung sowie das Schreiben von Regeln und sie stellt der Auto Deploy-Infrastruktur das Image-Profil zur Verfügung.

Voraussetzungen

Stellen Sie sicher, dass die Einrichtung, die Sie während des ersten Startvorgangs durchgeführt hatten, vorhanden ist.

Vorgehensweise

1. Überprüfen Sie, ob das Image-Profil und das Hostprofil für den Host immer noch verfügbar sind und ob der Host die Identifizierungsinformationen (Asset-Tag, IP-Adresse) hat, über die er während der vorherigen Startvorgänge verfügte.
2. Versetzen Sie den Host in den Wartungsmodus.

Hosttyp	Aktion
Der Host gehört zu einem DRS-Cluster.	vSphere DRS migriert virtuelle Maschinen auf entsprechende Hosts, wenn Sie den Host in den Wartungsmodus versetzen.
Der Host gehört nicht zu einem DRS-Cluster.	Sie müssen alle virtuelle Maschinen auf verschiedene Hosts migrieren und jeden Host in den Wartungsmodus versetzen.

3. Starten Sie den Host neu.

Der Host wird heruntergefahren. Wenn der Host neu gestartet wird, verwendet er das vom Auto Deploy-Server bereitgestellte Image-Profil. Der Auto Deploy-Server wendet auch das Hostprofil an, das auf dem vCenter Server-System gespeichert ist.

Erneutes Bereitstellen eines Hosts mit einem neuen Image-Profil

Sie können den Host mithilfe eines neuen Image-Profils, eines Hostprofils oder eines vCenter Server-Speicherorts erneut bereitstellen, indem Sie die Regel für den Host ändern und einen Vorgang zum Testen und zur Reparatur von Übereinstimmungen durchführen.

Es gibt mehrere Optionen zur erneuten Bereitstellung von Hosts.

- Wenn die VIBs, die Sie verwenden möchten, Live-Update unterstützen, können Sie einen `esxcli software vib`-Befehl verwenden. In diesem Fall müssen Sie außerdem den Regelsatz aktualisieren, damit er ein Image-Profil verwendet, das die neuen VIBs enthält.
- Während des Testens können Sie ein Image-Profil auf einen einzelnen Host anwenden, indem Sie das `Apply-EsxImageProfile`-cmdlet verwenden und den Host neu starten, damit die Änderung übernommen wird. Das `Apply-EsxImageProfile`-cmdlet aktualisiert die Verbindung zwischen dem Host und dem Image-Profil, installiert jedoch keine VIBs auf dem Host.
- Verwenden Sie in allen anderen Fällen diese Vorgehensweise.

Voraussetzungen

- Erstellen Sie das Image-Profil, mit dem Sie den Host starten möchten. Verwenden Sie die Image Builder PowerCLI, die in „Verwenden von vSphere ESXi Image Builder“, auf Seite 149 behandelt wird.
- Stellen Sie sicher, dass die Einrichtung, die Sie während des ersten Startvorgangs durchgeführt hatten, vorhanden ist.

Vorgehensweise

1. Führen Sie an der PowerShell-Eingabeaufforderung das `Connect-VIServer`-PowerCLI-cmdlet aus, um eine Verbindung zu dem vCenter Server-System herzustellen, bei dem Auto Deploy registriert ist.

   ```
   Connect-VIServer myVCServer
   ```

   Das cmdlet gibt möglicherweise eine Serverzertifikatswarnung zurück. Stellen Sie in einer Produktionsumgebung sicher, dass keine Serverzertifikatswarnungen ausgegeben werden. In einer Entwicklungsumgebung können Sie die Warnung ignorieren.

2. Ermitteln Sie den Speicherort eines öffentlichen Software-Depots, das das Image-Profil enthält, das Sie verwenden möchten, oder definieren Sie mithilfe der Image Builder PowerCLI ein eigenes Image-Profil.

3. Führen Sie `Add-EsxSoftwareDepot` aus, um das Software-Depot mit dem Image-Profil zur PowerCLI-Sitzung hinzuzufügen.

Depottyp	Cmdlet
Remote-Depot	Führen Sie **`Add-EsxSoftwareDepot`** ***`URL_des_Depots`*** aus.
ZIP-Datei	a Laden Sie die ZIP-Datei in einen lokalen Dateipfad herunter oder erstellen Sie in der PowerCLI-Maschine einen lokalen Mount-Punkt. b Führen Sie **`Add-EsxSoftwareDepot C:\`*****`Dateipfad`*****`\`*****`Mein_Offline-Depot`*****`.zip`** aus.

4. Führen Sie `Get-EsxImageProfile` aus, damit eine Liste der Image-Profile angezeigt wird, und entscheiden Sie, welches Profil Sie verwenden möchten.

5. Führen Sie `Copy-DeployRule` aus und legen Sie den Parameter `ReplaceItem` fest, um die Regel zu ändern, die ein Image-Profil zu Hosts zuweist.

   Das folgende cmdlet ersetzt das aktuelle Image-Profil, das die Regel dem Host mit dem *Mein_neues_Image-Profil*-Profil zuweist. Nachdem das cmdlet beendet wurde, weist `myrule` den Hosts das neue Image-Profil zu. Die alte Version von `myrule` wird umbenannt und ausgeblendet.

   ```
   Copy-DeployRule myrule -ReplaceItem Mein_neues_Image-Profil
   ```

6. Testen und reparieren Sie die Regelübereinstimmung für jeden Host, auf dem Sie das Image bereitstellen möchten.

   Weitere Informationen hierzu finden Sie unter „Testen und Reparieren der Regelübereinstimmung“, auf Seite 96.

Wenn Sie nach der Übereinstimmungsreparatur die Hosts neu starten, stellt Auto Deploy die Hosts mit dem neuen Image-Profil bereit.

Aktualisieren Sie die Hostanpassung im vSphere Web Client

Wenn ein Host während eines vorherigen Starts eine Eingabeaufforderung benötigte, werden die Antworten auf dem vCenter Server gespeichert. Wenn Sie den Benutzer zur Eingabe neuer Informationen auffordern möchten, standardisieren Sie den Host.

Voraussetzungen

Hängen Sie ein Hostprofil an den Host an, der den Benutzer zur Eingabe auffordert.

Vorgehensweise

1. Migrieren Sie alle virtuellen Maschinen auf verschiedene Hosts und versetzen Sie den Host in den Wartungsmodus.

Hosttyp	Aktion
Der Host gehört zu einem DRS-Cluster.	vSphere DRS migriert virtuelle Maschinen auf entsprechende Hosts, wenn Sie den Host in den Wartungsmodus versetzen.
Der Host gehört nicht zu einem DRS-Cluster.	Sie müssen alle virtuellen Maschinen auf verschiedene Hosts migrieren und jeden Host in den Wartungsmodus versetzen.

2. Klicken Sie im vSphere Web Client mit der rechten Maustaste auf den Host und klicken Sie auf **Alle vCenter-Aktionen > Hostprofile > Beheben**, um die Hostprobleme zu beheben.
3. Geben Sie die Benutzereingabe ein, wenn Sie dazu aufgefordert werden.

   Sie können nun den Host dazu anweisen, den Wartungsmodus zu beenden.

Die Hostanpassung wird gespeichert. Beim nächsten Start wird die Hostanpassung auf den Host angewendet.

Verwenden von Auto Deploy für statusfreies Caching und statusorientierte Installationen

Die Funktion für statusfreies Caching von Auto Deploy ermöglicht die Zwischenspeicherung des Host-Image. Die Funktion für statusorientierte Installationen von Auto Deploy ermöglicht die Installation von Hosts über das Netzwerk. Nach dem ersten Netzwerkstart starten diese Hosts wie alle anderen ESXi-Hosts.

Die statusfreie Caching-Lösung ist in erster Linie für Situationen ausgelegt, in denen mehrere Hosts gleichzeitig gestartet werden. Das lokal zwischengespeicherte Image hilft bei der Vermeidung von Engpässen, wenn mehrere hundert Hosts gleichzeitig auf den Auto Deploy-Server zugreifen. Nach dem abgeschlossenen Startvorgang stellen die Hosts eine Verbindung mit Auto Deploy her und schließen das Setup ab.

Mit der Funktion für statusorientierte Installationen können Sie den Hosts über das Netzwerk das Image-Profil zur Verfügung stellen, ohne eigens die PXE-Startinfrastruktur einrichten zu müssen.

- Einführung in statusfreies Caching und statusorientierte Installationen auf Seite 102

  Sie können das Hostprofil „Konfiguration des System-Caches“ verwenden, um für Hosts die Funktionen „Statusfreies Caching“ und „Statusorientierte Installationen“ von Auto Deploy bereitzustellen.
- Grundlegende Informationen zu statusfreiem Caching und statusorientierter Installationen auf Seite 104

  Wenn Sie Auto Deploy mit statusfreiem Caching oder statusorientierten Installationen verwenden möchten, müssen Sie ein Hostprofil einrichten und anwenden sowie die Startreihenfolge festlegen.
- Einrichten von statusfreien Hosts für die Verwendung von Auto Deploy mit Caching auf Seite 105

  Sie können Ihr System so einrichten, dass Hosts mit Auto Deploy bereitgestellt werden, und die Hosts so konfigurieren, dass statusfreies Caching verwendet wird. Wenn der Auto Deploy-Server beim Start eines Hosts nicht verfügbar ist, verwendet der Host das im Cache befindliche Image.
- Aktivieren von statusorientierten Installationen für mit Auto Deploy bereitgestellten Hosts auf Seite 108

  Sie können Hosts mit Auto Deploy einrichten, um das Image auf Datenträger zwischenzuspeichern und das im Cache befindliche Image für nachfolgende Startvorgänge zu verwenden. Nachdem das Image zwischengespeichert wurde, fungieren die Hosts wie Hosts, auf denen ein Image installiert ist.

Einführung in statusfreies Caching und statusorientierte Installationen

Sie können das Hostprofil „Konfiguration des System-Caches“ verwenden, um für Hosts die Funktionen „Statusfreies Caching“ und „Statusorientierte Installationen“ von Auto Deploy bereitzustellen.

Beispiele für statusfreies Caching und statusorientierte Installationen

Mit Auto Deploy bereitgestellte Hosts speichern das Image im Cache (statusfreies Caching)

Richten Sie ein Hostprofil für statusfreies Caching ein und wenden Sie es an. Sie können das Image im Cache auf einer lokalen Festplatte, einer Remotefestplatte oder einem USB-Laufwerk speichern. Stellen Sie diesen Host weiterhin mit Auto Deploy bereit. Wenn der Auto Deploy-Server nicht mehr verfügbar ist, weil beispielsweise Hunderte von Hosts versuchen, gleichzeitig auf ihn zuzugreifen, startet der Host aus dem Cache. Der Host versucht nach dem Starten, den Auto Deploy-Server zu erreichen, um die Konfiguration abzuschließen.

Mit Auto Deploy bereitgestellte Hosts werden statusorientierte Hosts

Richten Sie ein Hostprofil für statusorientierte Installation ein und wenden Sie es an. Wenn Sie einen Host mit Auto Deploy bereitstellen, wird das Image auf der lokalen Festplatte, einer Remotefestplatte oder einem USB-Laufwerk installiert. Bei nachfolgenden Starts wird von der Festplatte gestartet. Der Host verwendet Auto Deploy nicht mehr.

Vorbereitung

Entscheiden Sie, wie das System konfiguriert wird, und geben Sie die Startreihenfolge an, um erfolgreich statusfreies Caching oder statusorientierte Installationen zu verwenden.

Tabelle 4-7. Vorbereitung für statusfreies Caching oder statusorientierte Installationen

Anforderung oder Entscheidung	Beschreibung
Entscheidung über das Überschreiben der VMFS-Partition	Wenn Sie ESXi mithilfe des interaktiven Installationsprogramms installieren, werden Sie gefragt, ob Sie einen bestehenden VMFS-Datenspeicher überschreiben möchten. Das Hostprofil „Konfiguration des System-Caches“ bietet eine Option zum Überschreiben von bestehenden VMFS-Partitionen. Die Option wird nicht angezeigt, wenn Sie das Hostprofil für die Verwendung eines USB-Laufwerks einrichten.
Entscheidung über das Erfordernis der Hochverfügbarkeit	Wenn Sie Auto Deploy mit statusfreiem Caching verwenden, können Sie eine hochverfügbare Auto Deploy-Umgebung aufsetzen, um zu gewährleisten, dass virtuelle Maschinen auf neu bereitgestellte Hosts migriert werden und die Umgebung vSphere Distributed Switch auch unterstützt, wenn das vCenter Server-System vorübergehend nicht verfügbar ist.
Einrichten der Startreihenfolge	Die von Ihnen für Ihre Hosts festgelegte Startreihenfolge hängt von den Funktionen ab, die Sie benutzen wollen. ■ Um Auto Deploy mit statusfreiem Caching einzurichten, konfigurieren Sie Ihren Host so, dass er zunächst den Start aus dem Netzwerk und dann von der Festplatte versucht. Wenn der Auto Deploy-Server nicht verfügbar ist, startet der Host mit dem Cache. ■ Um Auto Deploy für statusorientiertes Installieren auf Hosts einzurichten, die derzeit keine startfähige Festplatte haben, konfigurieren Sie Ihre Hosts so, dass sie erst von der Festplatte und dann aus dem Netzwerk starten. HINWEIS Wenn Sie ein startfähiges Image auf der Festplatte haben, konfigurieren Sie die Hosts für einen einmaligen PXE-Start und richten Sie den Host mit Auto Deploy so ein, dass er ein Hostprofil verwendet, das statusorientierte Installationen festlegt.

Statusfreies Caching und Verlust der Konnektivität

Wenn die ESXi-Hosts, auf denen Ihre virtuellen Maschinen laufen, die Konnektivität mit dem Auto Deploy-Server, dem vCenter Server-System oder beiden verlieren, gelten einige Einschränkungen für den nächsten Neustart des Hosts.

- Wenn vCenter Server verfügbar ist, aber der Auto Deploy-Server nicht, verbinden sich Hosts nicht automatisch mit dem vCenter Server-System. Sie können die Hosts manuell mit vCenter Server verbinden oder warten, bis der Auto Deploy-Server wieder verfügbar ist.
- Wenn vCenter Server und Auto Deploy nicht verfügbar sind, können Sie mit jedem ESXi-Host mithilfe des vSphere Client eine Verbindung herstellen und jedem Host virtuelle Maschinen hinzufügen.
- Wenn vCenter Server nicht verfügbar ist, funktioniert vSphere DRS nicht. Der Auto Deploy-Server kann dem vCenter Server keine Hosts hinzufügen. Sie können mit jedem ESXi-Host mithilfe des vSphere Client eine Verbindung herstellen und jedem Host virtuelle Maschinen hinzufügen.
- Wenn Sie Änderungen an Ihrer Einrichtung vornehmen, während die Verbindung unterbrochen ist, gehen diese Änderungen verloren, wenn die Verbindung mit dem Auto Deploy-Server wiederhergestellt wird.

Grundlegende Informationen zu statusfreiem Caching und statusorientierter Installationen

Wenn Sie Auto Deploy mit statusfreiem Caching oder statusorientierten Installationen verwenden möchten, müssen Sie ein Hostprofil einrichten und anwenden sowie die Startreihenfolge festlegen.

Wenn Sie ein Hostprofil anwenden, das das Caching auf einen Host aktiviert, partitioniert Auto Deploy die angegebene Festplatte. Was als Nächstes passiert, hängt davon ab, wie Sie das Hostprofil einrichten und wie Sie die Startreihenfolge auf dem Host festlegen.

- Auto Deploy legt das Image im Cache ab, wenn Sie das Hostprofil anwenden, wenn im Hostprofil die Option **Statusfreies Caching auf dem Host aktivieren** ausgewählt ist. Es ist kein Neustart erforderlich. Wenn Sie später neu starten, verwendet der Host weiterhin die Auto Deploy-Infrastruktur, um das Image abzurufen. Wenn der Auto Deploy-Server nicht verfügbar ist, verwendet der Host das im Cache befindliche Image.
- Auto Deploy installiert das Image, wenn **Statusorientierte Installationen auf dem Host aktivieren** im Hostprofil der System-Cache-Konfiguration ausgewählt ist. Wenn Sie den Host neu starten, wird der Host von der Festplatte gestartet, genauso wie ein Host, der mit dem Installationsprogramm bereitgestellt wurde. Auto Deploy stellt den Host nicht mehr bereit.

Sie können das Hostprofil von einem vSphere Web Client anwenden oder eine Auto Deploy PowerCLI-Regel definieren, die auf das Hostprofil angewendet wird.

Verwenden des vSphere Web Client zum Einrichten von Auto Deploy für statusfreies Caching oder statusorientierte Installationen

Sie können ein Hostprofil auf einem Referenzhost erstellen und das Hostprofil auf weitere Hosts oder einen vCenter Server-Ordner- bzw. -Cluster anwenden. Das Ergebnis ist der folgende Workflow.

1. Sie stellen einen Host mit Auto Deploy bereit und bearbeiten das Hostprofil „Konfiguration des System-Image-Caches" für diesen Host.
2. Sie versetzen mindestens einen Zielhost in den Wartungsmodus, wenden das Hostprofil auf jeden Host an und weisen den Host an, den Wartungsmodus zu beenden.
3. Was als Nächstes passiert, hängt davon ab, welches Hostprofil Sie ausgewählt haben.
   - Wenn das Hostprofil statusfreies Caching aktiviert, wird das Image im Cache der Festplatte gespeichert. Es ist kein Neustart erforderlich.
   - Wenn das Hostprofil die statusorientierte Installation aktiviert hat, wird das Image installiert. Wenn Sie einen Neustart durchführen, verwendet der Host das installierte Image.
4. Ein Neustart ist erforderlich, damit die Änderungen wirksam werden können.

Verwenden von PowerCLI zum Einrichten von Auto Deploy für statusfreies Caching oder statusorientierte Installationen

Sie können ein Hostprofil für einen Referenzhost erstellen und eine Auto Deploy PowerCLI-Regel definieren, die das Hostprofil auf andere Zielhosts anwendet. Das Ergebnis ist der folgende Workflow.

1. Sie stellen eine Referenz mit Auto Deploy bereit und erstellen ein Hostprofil, um eine Form des Cachings zu aktivieren.
2. Sie definieren eine Regel, die weitere Hosts mit Auto Deploy bereitstellt und die das Hostprofil des Referenzhosts auf diese Hosts anwendet.

3 Auto Deploy stellt jedem Host das neue Image-Profil bereit. Die genaue Auswirkung der Anwendung des Hostprofils hängt vom ausgewählten Hostprofil ab.

- Bei statusorientierten Installationen geht Auto Deploy wie folgt vor:
  - Während des ersten Starts installiert Auto Deploy das Image auf dem Host.
  - Bei nachfolgenden Startvorgängen startet der Host von der Festplatte aus. Auto Deploy ist nicht mehr beteiligt.
- Bei statusfreiem Caching geht Auto Deploy wie folgt vor:
  - Beim ersten Start wird der Host mit Auto Deploy bereitgestellt und das Image gecacht.
  - Während nachfolgenden Startvorgängen stellt Auto Deploy den Host bereit. Wenn Auto Deploy nicht verfügbar ist, startet der Host vom gecachten Image aus. Die Einrichtung kann jedoch erst abgeschlossen werden, wenn der Host den Auto Deploy-Server erreichen kann.

Einrichten von statusfreien Hosts für die Verwendung von Auto Deploy mit Caching

Sie können Ihr System so einrichten, dass Hosts mit Auto Deploy bereitgestellt werden, und die Hosts so konfigurieren, dass statusfreies Caching verwendet wird. Wenn der Auto Deploy-Server beim Start eines Hosts nicht verfügbar ist, verwendet der Host das im Cache befindliche Image.

Ein Host, der für statusfreies Caching eingerichtet ist, verwendet das im Cache befindliche Image nur, wenn der Auto Deploy-Server beim Start des Hosts nicht verfügbar ist. In allen anderen Situationen wird der Host mit Auto Deploy bereitgestellt. Wenn Sie die Regel ändern, die ein Image-Profil auf den Host anwendet, und einen Vorgang zum Testen und Reparieren von Übereinstimmungen durchführen, stellt Auto Deploy für den Host das neue Image bereit und das neue Image wird in den Cache eingelesen.

Richten Sie eine hochverfügbare Auto Deploy-Infrastruktur ein, um zu garantieren, dass virtuelle Maschinen auf den Host migriert werden, wenn der Host neu startet. Da vCenter Server dem Host virtuelle Maschinen zuweist, muss vCenter Server verfügbar sein. Weitere Informationen hierzu finden Sie unter „Einrichten einer hochverfügbaren Auto Deploy-Infrastruktur", auf Seite 125.

Sie können Ihre Umgebung für das statusfreie Caching einrichten, indem Sie die Hostprofile direkt übernehmen oder PowerCLI-Regeln anwenden.

Tabelle 4-8. Einrichten von Hosts für statusfreies Caching oder statusorientierte Installationen

Workflow	Statusfreies Caching	Statusorientierte Installation
Direktes Anwenden des Hostprofils	Wenden Sie das Hostprofil entweder auf individuelle Hosts oder auf alle Hosts in einem Ordner oder Cluster an. Weitere Informationen hierzu finden Sie unter „Konfigurieren eines Hostprofils für die Verwendung von statusfreiem Caching", auf Seite 106.	Wenden Sie das Hostprofil entweder auf individuelle Hosts oder auf alle Hosts in einem Ordner oder Cluster an. Weitere Informationen hierzu finden Sie unter „Konfigurieren eines Hostprofils für das Aktivieren von statusorientierten Installationen", auf Seite 108.
Schreiben und Anwenden von PowerCLI-Regeln	Richten Sie einen Referenzhost mit einem Hostprofil ein, in dem das gewünschte Caching festgelegt ist. Schreiben Sie eine Auto Deploy PowerCLI-Regel, die den Host bereitstellt und ein Hostprofil anwendet, das für statusfreies Caching ausgelegt ist. Weitere Informationen hierzu finden Sie unter „Erstellen einer Regel und Zuweisen eines Hostprofils zu Hosts", auf Seite 94.	Richten Sie einen Referenzhost mit einem Hostprofil ein, in dem das gewünschte Caching festgelegt ist. Schreiben Sie eine Auto Deploy PowerCLI-Regel, die den Host bereitstellt und ein Hostprofil anwendet, das für statusorientierte Installationen ausgelegt ist. Weitere Informationen hierzu finden Sie unter „Erstellen einer Regel und Zuweisen eines Hostprofils zu Hosts", auf Seite 94.

Vorbereiten auf Auto Deploy mit statusfreiem Caching

Bevor Sie einen Host, der statusfreies Caching verwendet, mit Auto Deploy bereitstellen können, müssen Sie sicherstellen, dass Ihre Umgebung für Auto Deploy eingerichtet ist, Auto Deploy-PowerCLI-Regeln vorbereiten und die Host-Startreihenfolge festlegen.

Voraussetzungen

- Definieren Sie die Festplatte, die für das Caching verwendet werden soll, und legen Sie fest, ob der Caching-Prozess eine vorhandene VMFS-Partition überschreiben soll.
- Schützen Sie in Produktionsumgebungen das vCenter Server-System und den Auto Deploy-Server, indem Sie sie in eine hoch verfügbare Umgebung aufnehmen. Das Vorhandensein von vCenter Server in einem Verwaltungscluster gewährleistet, dass vDS- und VM-Migrationen möglich sind. Schützen Sie, falls möglich, weitere Elemente Ihrer Infrastruktur. Weitere Informationen hierzu finden Sie unter „Einrichten einer hochverfügbaren Auto Deploy-Infrastruktur“, auf Seite 125.

Vorgehensweise

1 Richten Sie Ihre Umgebung für Auto Deploy ein und installieren Sie PowerCLI.

  Weitere Informationen hierzu finden Sie unter „Vorbereitung für vSphere Auto Deploy“, auf Seite 87.

2 Stellen Sie sicher, dass eine Festplatte mit mindestens 1 GB freiem Speicherplatz zur Verfügung steht.

  Falls die Festplatte noch nicht partitioniert ist, erfolgt die Partitionierung bei Anwendung des Hostprofils.

3 Richten Sie den Host so ein, dass er zuerst versucht, vom Netzwerk und dann von der Festplatte zu starten, falls das Starten vom Netzwerk fehlschlägt.

  Weitere Informationen finden Sie in der Dokumentation Ihres Hardwareanbieters.

Weiter

Richten Sie ein Hostprofil für statusfreies Caching ein. In den meisten Fällen richten Sie das Hostprofil auf einem Referenzhost ein und wenden dieses Hostprofil auf andere Hosts an.

Konfigurieren eines Hostprofils für die Verwendung von statusfreiem Caching

Wenn ein Host zur Verwendung von statusfreiem Caching eingerichtet ist, verwendet der Host ein im Cache befindliches Image, wenn der Auto Deploy-Server nicht verfügbar ist. Sie müssen ein Hostprofil konfigurieren, um statusfreies Caching zu verwenden. Sie können dieses Hostprofil auf andere Hosts anwenden, die Sie für statusfreies Caching einrichten möchten.

Sie können das Hostprofil auf einem einzelnen Host konfigurieren, den Sie zur Verwendung von Caching einrichten möchten. Sie können auch ein Hostprofil, das Caching verwendet, auf einem Referenzhost erstellen und dieses Hostprofil auf andere Hosts anwenden.

Voraussetzungen

Bereiten Sie den Host für statusfreies Caching vor. Weitere Informationen hierzu finden Sie unter „Vorbereiten auf Auto Deploy mit statusfreiem Caching“, auf Seite 106.

Vorgehensweise

1 Erstellen Sie im vSphere Web Client ein Hostprofil.

  Weitere Informationen finden Sie in der Dokumentation *Hostprofile*.

2 Wählen Sie das Hostprofil aus und klicken Sie auf **Hostprofil bearbeiten**.

3 Lassen Sie den Namen und die Beschreibung unverändert und klicken Sie auf **Weiter**.

4 Klicken Sie auf **Erweiterte Konfigurationseinstellungen** und klicken Sie auf den Ordner **Konfiguration des System-Image-Caches**.

5 Klicken Sie auf das Symbol **Konfiguration des System-Image-Caches**.

6 Nehmen Sie Ihre Auswahl im Dropdown-Menü „Profileinstellungen für System-Image-Cache“ vor.

Option	Beschreibung
Statusfreies Caching auf dem Host aktivieren	Nimmt eine Zwischenspeicherung des Image auf Festplatte vor.
Statusfreies Caching für eine USB-Festplatte auf dem Host aktivieren	Nimmt eine Zwischenspeicherung des Image auf der mit dem Host verbundenen USB-Festplatte vor.

7 Wenn Sie **Statusfreies Caching auf dem Host aktivieren** auswählen, geben Sie die Informationen über die zu verwendende Festplatte an.

Option	Beschreibung
Argumente für die erste Festplatte	Standardmäßig versucht das System, eine bestehende ESXi-Installation zu ersetzen und anschließend auf die lokale Festplatte zu schreiben. Sie können im Feld **Argumente für erste Festplatte** eine kommagetrennte Liste der zu verwendenden Festplatten in der Reihenfolge ihrer Priorität festlegen. Sie können mehr als eine Festplatte angeben. Verwenden Sie **`esx`** für die erste Festplatte, auf der ESX installiert ist, verwenden Sie Modell- und Anbieterinformationen oder geben Sie den Namen des VMkernel-Gerätetreibers ein. Damit das System z. B. zuerst nach einer Festplatte mit dem Modellnamen ST3120814A sucht, zweitens nach einer beliebigen Festplatte, die den Treiber mptsas verwendet, und drittens nach der lokalen Festplatte, legen Sie **`ST3120814A,mptsas,local`** als Wert für dieses Feld fest. Die erste Festplatteneinstellung im Hostprofil gibt die Suchreihenfolge an, die festlegt, welche Festplatte für den Cache verwendet wird. Die Suchreihenfolge wird als kommagetrennte Werteliste angegeben. Die Standardeinstellung **`esx,local`** gibt an, dass Auto Deploy zuerst nach einer vorhandenen Cache-Festplatte suchen soll. Die Cache-Festplatte wird als Festplatte mit einem vorhandenen ESXi-Softwareimage identifiziert. Wenn Auto Deploy keine vorhandene Cache-Festplatte findet, wird nach einem vorhandenen lokalen Festplattengerät gesucht. Bei der Suche nach einer verfügbaren Festplatte verwendet Auto Deploy die erste leere Festplatte, die keine vorhandene VMFS-Partition enthält. Sie können das Argument für die erste Festplatte nur zum Festlegen der Suchreihenfolge angeben. Es kann keine Festplatte explizit festgelegt werden. Sie können z. B. nicht eine bestimmte LUN in einem SAN festlegen.
Aktivieren Sie diese Option, um die VMFS-Volumes auf der ausgewählten Festplatte zu überschreiben	Wenn Sie auf dieses Kontrollkästchen klicken, überschreibt das System bestehende VMFS-Volumes, wenn der Festplattenspeicher nicht ausreicht, um Image, Image-Profil und Hostprofil zu speichern.

8 Klicken Sie auf **Beenden**, um die Konfiguration des Hostprofils abzuschließen.

9 Wenden Sie das Hostprofil mit dem vSphere Web Client oder vSphere PowerCLI an.

Option	Beschreibung
vSphere Web Client	Verwenden Sie die Benutzeroberfläche für Hostprofile von vSphere Web Client. Weitere Informationen finden Sie in der Dokumentation *Hostprofile*.
vSphere PowerCLI	Weitere Informationen hierzu finden Sie unter „Erstellen einer Regel und Zuweisen eines Hostprofils zu Hosts“, auf Seite 94.

Aktivieren von statusorientierten Installationen für mit Auto Deploy bereitgestellten Hosts

Sie können Hosts mit Auto Deploy einrichten, um das Image auf Datenträger zwischenzuspeichern und das im Cache befindliche Image für nachfolgende Startvorgänge zu verwenden. Nachdem das Image zwischengespeichert wurde, fungieren die Hosts wie Hosts, auf denen ein Image installiert ist.

Vorbereiten von mit Auto Deploy bereitgestellten Hosts für statusorientierte Installationen

In einigen Situationen ist es nützlich, Hosts mit Auto Deploy bereitzustellen und alle anschließenden Startvorgänge von der Festplatte aus durchzuführen. Dieser Ansatz wird als „Statusorientierte Installationen" bezeichnet.

Voraussetzungen

Definieren Sie die Festplatte, die zum Speichern des Images verwendet werden soll, und legen Sie fest, ob das neue Image eine vorhandene VMFS-Partition überschreiben soll.

Vorgehensweise

1 Richten Sie Ihre Umgebung für Auto Deploy ein und installieren Sie PowerCLI.

   Weitere Informationen hierzu finden Sie unter „Vorbereitung für vSphere Auto Deploy", auf Seite 87.

2 Stellen Sie sicher, dass eine Festplatte mit mindestens 1 GB freiem Speicherplatz zur Verfügung steht.

   Falls die Festplatte nicht partitioniert ist, erfolgt die Partitionierung bei Anwendung des Hostprofils.

3 Richten Sie den Host so ein, dass er von der Festplatte startet.

   Weitere Informationen finden Sie in der Dokumentation Ihres Hardwareanbieters.

Konfigurieren eines Hostprofils für das Aktivieren von statusorientierten Installationen

Um einen Host einzurichten, der mit Auto Deploy zum Starten von einer Festplatte bereitgestellt wurde, müssen Sie ein Hostprofil konfigurieren. Sie können dieses Hostprofil auf andere Hosts anwenden, die Sie für statusorientierte Installationen einrichten möchten.

Sie können das Hostprofil auf einem einzelnen Host konfigurieren. Sie können auch ein Hostprofil auf einem Referenzhost erstellen und dieses Hostprofil auf andere Hosts anwenden.

Voraussetzungen

Stellen Sie sicher, dass der Host für Auto Deploy konfiguriert ist und die anderen Voraussetzungen für statusorientierte Installationen erfüllt. Weitere Informationen hierzu finden Sie unter „Vorbereiten von mit Auto Deploy bereitgestellten Hosts für statusorientierte Installationen", auf Seite 108.

Vorgehensweise

1 Erstellen Sie im vSphere Web Client ein Hostprofil.

   Weitere Informationen finden Sie in der Dokumentation *Hostprofile*.

2 Wenn das Hostprofilobjekt angezeigt wird, klicken Sie auf das Symbol „Hostprofileinstellungen bearbeiten".

3 Lassen Sie den Namen und die Beschreibung unverändert und klicken Sie auf **Weiter**.

4 Klicken Sie auf **Erweiterte Konfigurationseinstellungen** und klicken Sie auf den Ordner **Konfiguration des System-Image-Caches**.

5 Klicken Sie auf das Symbol **Konfiguration des System-Image-Caches**.

6 Nehmen Sie Ihre Auswahl im Dropdown-Menü „Profileinstellungen für System-Image-Cache“ vor.

Option	Beschreibung
statusorientierte Installationen auf dem Host aktivieren	Nimmt eine Zwischenspeicherung des Image auf Festplatte vor.
statusorientierte Installationen für eine USB-Festplatte auf dem Host aktivieren	Nimmt eine Zwischenspeicherung des Image auf der mit dem Host verbundenen USB-Festplatte vor.

7 Wenn Sie **statusorientierte Installationen auf dem Host aktivieren** auswählen, legen Sie die Informationen über die zu verwendende Festplatte fest.

Option	Beschreibung
Argumente für die erste Festplatte	Standardmäßig versucht das System, eine bestehende ESXi-Installation zu ersetzen und anschließend auf die lokale Festplatte zu schreiben. Sie können im Feld **Argumente für erste Festplatte** eine kommagetrennte Liste der zu verwendenden Festplatten in der Reihenfolge ihrer Priorität festlegen. Sie können mehr als eine Festplatte angeben. Verwenden Sie **`esx`** für die erste Festplatte, auf der ESX installiert ist, verwenden Sie Modell- und Anbieterinformationen oder geben Sie den Namen des VMkernel-Gerätetreibers ein. Damit das System z. B. zuerst nach einer Festplatte mit dem Modellnamen ST3120814A sucht, zweitens nach einer beliebigen Festplatte, die den Treiber mptsas verwendet, und drittens nach der lokalen Festplatte, legen Sie **`ST3120814A,mptsas,local`** als Wert für dieses Feld fest. Die erste Festplatteneinstellung im Hostprofil gibt die Suchreihenfolge an, die festlegt, welche Festplatte für den Cache verwendet wird. Die Suchreihenfolge wird als kommagetrennte Werteliste angegeben. Die Standardeinstellung **`esx,local`** gibt an, dass Auto Deploy zuerst nach einer vorhandenen Cache-Festplatte suchen soll. Die Cache-Festplatte wird als Festplatte mit einem vorhandenen ESXi-Softwareimage identifiziert. Wenn Auto Deploy keine vorhandene Cache-Festplatte findet, wird nach einem vorhandenen lokalen Festplattengerät gesucht. Bei der Suche nach einer verfügbaren Festplatte verwendet Auto Deploy die erste leere Festplatte, die keine vorhandene VMFS-Partition enthält. Sie können das Argument für die erste Festplatte nur zum Festlegen der Suchreihenfolge angeben. Es kann keine Festplatte explizit festgelegt werden. Sie können z. B. nicht eine bestimmte LUN in einem SAN festlegen.
Aktivieren Sie diese Option, um die VMFS-Volumes auf der ausgewählten Festplatte zu überschreiben	Wenn Sie auf dieses Kontrollkästchen klicken, überschreibt das System bestehende VMFS-Volumes, wenn der Festplattenspeicher nicht ausreicht, um Image, Image-Profil und Hostprofil zu speichern.

8 Klicken Sie auf **Beenden**, um die Konfiguration des Hostprofils abzuschließen.

9 Wenden Sie das Hostprofil mit dem vSphere Web Client oder vSphere PowerCLI an.

Option	Beschreibung
vSphere Web Client	Wenn Sie das Hostprofil auf einzelne Hosts anwenden möchten, verwenden Sie die Benutzeroberfläche für Hostprofile von vSphere Web Client. Weitere Informationen finden Sie in der Dokumentation *Hostprofile*.
vSphere PowerCLI	Informationen zum Anwenden des Hostprofils auf einen oder mehrere Hosts mithilfe von PowerCLI finden Sie unter „Erstellen einer Regel und Zuweisen eines Hostprofils zu Hosts“, auf Seite 94.

Einrichten eines Auto Deploy-Referenzhosts

In einer Umgebung, in der kein Zustand auf dem Host gespeichert wird, hilft Ihnen ein Referenzhost beim Einrichten mehrerer Hosts mit derselben Konfiguration. Sie konfigurieren den Referenzhost mit Protokollierung, Core-Dump und anderen gewünschten Einstellungen, speichern das Hostprofil und schreiben eine Regel, die bei Bedarf das Hostprofil auf andere Hosts anwendet.

Sie können Speicher, Netzwerk und Sicherheitseinstellungen auf dem Referenzhost konfigurieren und Dienste, z. B. syslog und NTP, einrichten.

Grundlegende Informationen zur Einrichtung von Referenzhosts

Ein gut entworfener Referenzhost stellt Verbindungen zu allen Diensten, z. B. syslog, NTP usw., her. Die Einrichtung des Referenzhosts kann auch Sicherheits-, Speicher-, Netzwerk- und ESXi Dump Collector-Funktionen umfassen. Sie können ein solches Hostsetup auf andere Hosts mithilfe von Hostprofilen anwenden.

Die genaue Einrichtung Ihres Referenzhosts hängt von Ihrer Umgebung ab, Sie können aber die folgende Anpassung in Erwägung ziehen.

NTP-Server-Einrichtung

Wenn Sie Protokollierungsinformationen in großen Umgebungen erfassen, müssen Sie sicherstellen, dass die Protokollierungszeiten koordiniert sind. Legen Sie für den Referenzhost fest, dass er den NTP-Server in Ihrer Umgebung verwendet, auf den alle Hosts zugreifen können. Durch Ausführen des `vicfg-ntp`-Befehls können Sie einen NTP-Server angeben. Sie können den NTP-Dienst für einen Host mit dem Befehl `vicfg-ntp` oder über den vSphere Web Client starten und beenden.

Syslog Server-Einrichtung

Auf allen ESXi-Hosts wird ein syslog-Dienst (`vmsyslogd`) ausgeführt, der Meldungen vom VMkernel und anderen Systemkomponenten in einer Datei protokolliert. Sie können den Protokoll-Host angeben und Speicherort, Rotation, Größe und andere Attribute des Protokolls durch Ausführen des vCLI-Befehls `esxcli system syslog` oder mithilfe des vSphere Web Client verwalten. Die Einrichtung der Protokollierung auf einem Remotehost ist besonders wichtig für Hosts, die mit Auto Deploy bereitgestellt wurden und über keinen lokalen Speicher verfügen. Optional können Sie den vSphere Syslog Collector installieren, um Protokolle von allen Hosts zu erfassen.

Core-Dump-Einrichtung

Sie können Ihren Referenzhost so einrichten, dass er Core-Dumps an eine freigegebene SAN-LUN sendet, oder Sie können ESXi Dump Collector in Ihrer Umgebung installieren und den Referenzhost für die Verwendung von ESXi Dump Collector konfigurieren. Siehe „Konfigurieren des ESXi Dump Collectors mit ESXCLI“, auf Seite 112. Sie können ESXi Dump Collector entweder mithilfe der vCenter Server-Installationsmedien installieren oder den ESXi Dump Collector verwenden, der in der vCenter Server Appliance enthalten ist. Nach Abschluss der Installation wird der VMkernel-Arbeitsspeicher an den angegebenen Netzwerkserver gesendet, sobald das System einen kritischen Fehler feststellt.

Einrichtung der Sicherheit

In den meisten Bereitstellungen müssen alle Hosts, die Sie mit Auto Deploy bereitstellen, dieselben Sicherheitseinstellungen haben. Nehmen Sie alle Anpassungen an Ihrem Referenzhost vor. Sie können z. B. die Firewall so einrichten, dass bestimmte Dienste auf das ESXi-System zugreifen dürfen. Weitere Informationen finden Sie in der Dokumentation zu *vSphere-Sicherheit*.

Die Einrichtung der Sicherheit umfasst auch gemeinsam genutzte Benutzerzugriffseinstellungen für alle Hosts. Sie erreichen einen vereinheitlichten Benutzerzugriff durch die Einrichtung Ihres Referenzhosts für die Verwendung von Active Directory.

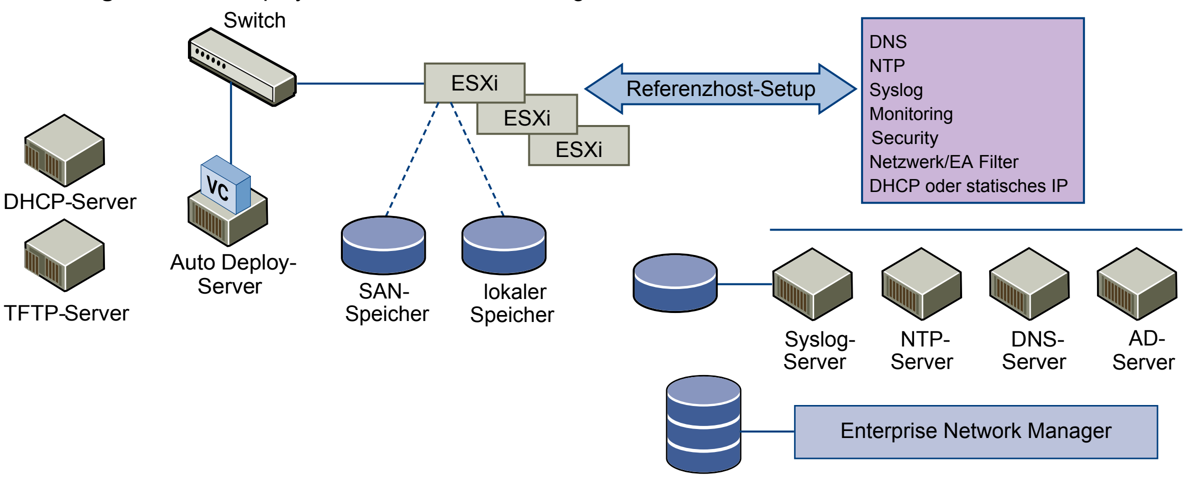
HINWEIS Wenn Sie Active Directory mithilfe von Hostprofilen einrichten, werden die Kennwörter nicht geschützt. Verwenden Sie den vSphere-Authentifizierungsdienst zum Einrichten von Active Directory, um zu verhindern, dass die Active Directory-Kennwörter freigelegt werden.

Netzwerk- und Speichereinrichtung

Wenn Sie einen Satz von Netzwerk- und Speicherressourcen für die Verwendung durch Hosts reservieren, die mit Auto Deploy bereitgestellt wurden, können Sie Ihren Referenzhost so einrichten, dass er diese Ressourcen verwendet.

In sehr großen Bereitstellungen unterstützt die Referenzhost-Einrichtung einen Enterprise Network Manager, der alle Informationen von den verschiedenen Überwachungsdiensten, die in der Umgebung ausgeführt werden, erfasst.

Abbildung 4-4. Auto Deploy-Referenzhost-Einrichtung



„Konfigurieren eines Auto Deploy-Referenzhosts“, auf Seite 112 beschreibt, wie Sie diese Einrichtung durchführen.

In dem Video „Auto Deploy Reference Hosts“ erhalten Sie Informationen zur Referenzhost-Einrichtung:



Auto Deploy Reference Hosts (http://link.brightcove.com/services/player/bcpid2296383276001?bctid=ref:video_auto_deploy_reference_hosts)

Konfigurieren eines Auto Deploy-Referenzhosts

vSphere ermöglicht es Ihnen, einen Referenzhost mithilfe des vSphere Web Client, mithilfe von vCLI oder mithilfe von Hostprofilen zu konfigurieren.

Sie können zum Einrichten eines Referenzhosts den Ansatz verwenden, den Ihnen am besten passt.

vSphere Web Client
Der vSphere Web Client unterstützt das Einrichten des Netzwerks, des Speichers, der Sicherheit und der meisten anderen Aspekte eines ESXi-Hosts. Richten Sie vom Referenzhost aus Ihre Umgebung ein und erstellen Sie ein Hostprofil zur Verwendung durch Auto Deploy.

vSphere-Befehlszeilen-schnittstelle
Sie können vCLI-Befehle zum Einrichten vieler Aspekte Ihres Hosts verwenden. vCLI eignet sich für das Konfigurieren vieler der Dienste in der vSphere-Umgebung. Zu den Befehlen gehören `vicfg-ntp` (Einrichten eines NTP-Servers), `esxcli system syslog` (Einrichten eines Syslog-Servers) und `esxcli network route` (Hinzufügen von Routen und das Einrichten der Standardroute). Weitere Informationen hierzu finden Sie unter „Konfigurieren des ESXi Dump Collectors mit ESXCLI“, auf Seite 112.

Hostprofile-Schnittstelle
Es wird empfohlen, mit vSphere Web Client oder vCLI einen Host einzurichten und von diesem Host ein Hostprofil zu erstellen. Sie können stattdessen die Schnittstelle „Hostprofile“ im vSphere Web Client verwenden und das Hostprofil speichern. Weitere Informationen hierzu finden Sie unter „Konfigurieren von Hostprofilen für einen Auto Deploy-Referenzhost mit dem vSphere Web Client“, auf Seite 113.

Konfigurieren des ESXi Dump Collectors mit ESXCLI

Ein Core-Dump bildet im Falle eines Hostausfalls den Zustand des Arbeitsspeichers ab. Standardmäßig wird ein Core-Dump auf der lokalen Festplatte gespeichert. Sie können den ESXi Dump Collector verwenden, um zwecks Fehlerbehebung Core-Dumps auf einem Netzwerkserver bereitzuhalten. ESXi Dump Collector ist besonders nützlich für Auto Deploy, wird jedoch für jeden ESXi-Host unterstützt. ESXi Dump Collector unterstützt weitere Anpassungen, darunter das Senden von Core-Dumps auf die lokale Festplatte.

Wenn Sie IPv6 verwenden möchten und sich sowohl der ESXi-Host als auch ESXi Dump Collector in derselben lokalen Verknüpfung befinden, können beide entweder IPv6-Adressen aus dem lokalen Verknüpfungsbereich oder IPv6-Adressen aus dem globalen Bereich nutzen.

Wenn Sie IPv6 verwenden möchten und der ESXi-Host und ESXi Dump Collector sich hingegen auf unterschiedlichen Hosts befinden, benötigen beide IPv6-Adressen aus dem globalen Bereich. Der Datenverkehr wird durch das standardmäßige IPv6-Gateway geleitet.

Voraussetzungen

- ESXi Dump Collector ist im vCenter Server-Verwaltungsknoten enthalten.
- Installieren Sie vCLI, wenn Sie den Host für die Verwendung von ESXi Dump Collector konfigurieren möchten. Bei der Fehlerbehebung können Sie stattdessen ESXCLI in der ESXi Shell verwenden.

Vorgehensweise

1 Richten Sie ein ESXi-System für die Verwendung von ESXi Dump Collector ein, indem Sie `esxcli system coredump` in der lokalen ESXi Shell ausführen oder vCLI verwenden.

```
esxcli system coredump network set --interface-name vmk0    --server-ip 10xx.xx.xx.xx --server-port 6500
```

Sie müssen eine VMkernel-Netzwerkkarte und die IP-Adresse sowie optional den Port des Servers, an den die Core-Dumps gesendet werden sollen, angeben. Sie können eine IPv4- oder eine IPv6-Adresse verwenden. Wenn Sie ein ESXi-System konfigurieren, das in einer virtuellen Maschine mit vSphere Standard Switch ausgeführt wird, müssen Sie einen VMkernel-Port im Promiscuous-Modus auswählen.

2 Aktiveren Sie ESXi Dump Collector.

```
esxcli system coredump network set --enable true
```

3 (Optional) Stellen Sie sicher, dass ESXi Dump Collector ordnungsgemäß konfiguriert ist.

```
esxcli system coredump network check
```

Der Host, auf dem Sie ESXi Dump Collector eingerichtet haben, ist so konfiguriert, dass er unter Verwendung der angegebenen VMkernel-Netzwerkkarte und des optionalen Ports Core-Dumps an den angegebenen Server sendet.

Weiter

- Erstellen Sie eine Regel, durch die das Hostprofil auf alle Hosts angewendet wird, die Sie mit den auf dem Referenzhost angegebenen Einstellungen bereitstellen möchten. Siehe „Erstellen einer Regel und Zuweisen eines Hostprofils zu Hosts“, auf Seite 94.
- Bei Hosts, die bereits mit Auto Deploy bereitgestellt wurden, führen Sie den Test durch und reparieren Sie die Übereinstimmungsvorgänge, um sie mit dem neuen Hostprofil zu versehen. Siehe „Testen und Reparieren der Regelübereinstimmung“, auf Seite 96.
- Schalten Sie noch nicht ausgestattete Hosts ein, um sie mit dem neuen Hostprofil auszustatten.

Konfigurieren von Hostprofilen für einen Auto Deploy-Referenzhost mit dem vSphere Web Client

Sie können Hostprofile in einem Referenzhost einrichten und die Hostprofileinstellungen auf alle anderen mit vSphere Auto Deploy bereitgestellten Hosts anwenden. Sie können entweder den Referenzhost konfigurieren und das Hostprofil exportieren oder bei kleinen Änderungen das Hostprofil direkt bearbeiten.

Voraussetzungen

Stellen Sie sicher, dass Sie auf einen vSphere Web Client zugreifen können, der eine Verbindung mit dem vCenter Server-System herstellen kann.

Vorgehensweise

1 Klicken Sie im vSphere Web Client auf **Regeln und Profile** und klicken Sie dann auf **Hostprofile**.

2 Klicken Sie für ein neues Profil auf **Profil vom Host erstellen** oder klicken Sie mit der rechten Maustaste auf ein Profil, das Sie ändern möchten, und wählen Sie **Hostprofil bearbeiten**.

3 Passen Sie Ihren Referenzhost mithilfe von vCLI, der Client-Benutzeroberfläche oder der Benutzeroberfläche für Hostprofile an.

Richtlinie	Beschreibung
ESXi Dump Collector	Richten Sie mithilfe des Befehls `esxcli system coredump` ESXi Dump Collector ein und speichern Sie das Hostprofil (Best Practice) oder konfigurieren Sie das Hostprofil direkt. Weitere Informationen hierzu finden Sie unter „Einrichten von Syslog über die Schnittstelle „Hostprofile" im vSphere Web Client", auf Seite 115.
Syslog	Richten Sie syslog für den Host mithilfe des Befehls `esxcli system syslog` ein. Speichern Sie das Hostprofil (Best Practice) oder konfigurieren Sie das Hostprofil direkt. Weitere Informationen hierzu finden Sie unter „Einrichten von Syslog über die Schnittstelle „Hostprofile" im vSphere Web Client", auf Seite 115.
NTP	Verwenden Sie zum Einrichten eines Hosts den vCLI-Befehl `vicfg-ntp` oder den vSphere Web Client. Wenn Sie den vSphere Web Client zum Starten des NTP-Servers verwenden, stellen Sie sicher, dass die Startrichtlinie für den NTP-Daemon entsprechend festgelegt ist. a Wählen Sie im vSphere Web Client den Host aus. b Wählen Sie die Registerkarte „Verwalten" und klicken Sie auf **Uhrzeitkonfiguration**. c Klicken Sie auf **Bearbeiten** und klicken Sie auf „NTP (Network Time Protocol) verwenden (NTP-Client aktivieren)". d Wählen Sie **Mit dem Host starten und beenden** als Startrichtlinie für den NTP-Dienst.
Sicherheit	Richten Sie mithilfe von vSphere Web Client oder der vCLI-Befehle die Firewall-Konfiguration, die Sicherheitskonfiguration, die Benutzerkonfiguration und die Konfiguration der Benutzergruppe für den Referenzhost ein. Weitere Informationen finden Sie in der Dokumentation zu *vSphere-Sicherheit*.
Netzwerk und Speicher	Richten Sie mithilfe von vSphere Web Client oder der vCLI-Befehle die Netzwerk- und Speicherrichtlinien für den Referenzhost ein.

4 Klicken Sie auf **OK**, um die Hostprofileinstellungen zu speichern.

Weiter

Erstellen Sie eine Regel, anhand der das Hostprofil für alle Hosts angewendet wird, die Sie mit den von Ihnen auf dem Referenzhost angegebenen Einstellungen bereitstellen möchten (siehe „Erstellen einer Regel und Zuweisen eines Hostprofils zu Hosts", auf Seite 94). Führen Sie einen Vorgang zum Testen und zur Reparatur von Übereinstimmungen durch.

Einrichten des ESXi Dump Collector über die Schnittstelle „Hostprofile" im vSphere Web Client

Sie können den ESXi Dump Collector für einen Referenzhost mithilfe von `esxcli` oder direkt in den Bereichen „Hostprofile" des vSphere Web Client einrichten. Sie können das Hostprofil exportieren und eine Regel schreiben, die das Profil auf alle Hosts anwendet, die über Auto Deploy bereitgestellt wurden.

Es wird empfohlen, die Hosts so einzurichten, dass sie ESXi Dump Collector mit dem Befehl `esxcli system coredump` verwenden und das Hostprofil speichern (Informationen hierzu unter „Konfigurieren des ESXi Dump Collectors mit ESXCLI", auf Seite 112). Wenn Sie lieber eine grafische Benutzeroberfläche verwenden, richten Sie ESXi Dump Collector über die Schnittstelle „Hostprofile" ein.

Voraussetzungen

Überprüfen Sie, ob mindestens eine Partition genügend Speicherkapazität für Core-Dumps von mehreren Hosts hat, die mithilfe von vSphere Auto Deploy bereitgestellt wurden.

Vorgehensweise

1 Klicken Sie im vSphere Web Client auf **Regeln und Profile** und klicken Sie dann auf **Hostprofile**.

2 Klicken Sie für ein neues Profil auf **Profil vom Host erstellen** oder klicken Sie mit der rechten Maustaste auf ein Profil, das Sie ändern möchten, und wählen Sie **Hostprofil bearbeiten**.

3 Lassen Sie den Namen und die Beschreibung unverändert und klicken Sie auf **Weiter**.

4 Wählen Sie **Netzwerkkonfiguration**.

5 Wählen Sie **Netzwerk-Coredump-Einstellungen**.

6 Klicken Sie auf das Kontrollkästchen **Aktiviert**.

7 Geben Sie die zu verwendende Host-Netzwerkkarte, die IP-Adresse des Netzwerk-Coredump-Servers und den Port des Netzwerk-Coredump-Servers an.

8 Klicken Sie auf **Beenden**, um die Hostprofileinstellungen zu speichern.

Weiter

- Erstellen Sie eine Regel, durch die das Hostprofil auf alle Hosts angewendet wird, die Sie mit den von Ihnen auf dem Referenzhost angegebenen Einstellungen bereitstellen möchten. Weitere Informationen hierzu finden Sie unter „Erstellen einer Regel und Zuweisen eines Hostprofils zu Hosts“, auf Seite 94.
- Bei Hosts, die bereits mit Auto Deploy bereitgestellt wurden, führen Sie die Übereinstimmungstests und die Reparaturvorgänge durch, um sie mit dem neuen Hostprofil zu versehen. Weitere Informationen hierzu finden Sie unter „Testen und Reparieren der Regelübereinstimmung“, auf Seite 96.
- Schalten Sie nicht bereitgestellte Hosts ein, um sie mit dem Hostprofil bereitzustellen.

Einrichten von Syslog über die Schnittstelle „Hostprofile“ im vSphere Web Client

Hosts, die mit Auto Deploy bereitgestellt wurden, verfügen in der Regel nicht über genügend lokalen Speicher zum Speichern der Systemprotokolle. Sie können für diese Hoste einen Remote-Syslog-Server angeben, indem Sie einen Referenzhost einrichten, das Hostprofil speichern und dieses Hostprofil bei Bedarf für andere Hosts übernehmen.

Es wird empfohlen, den Syslog-Server auf dem Referenzhost mit dem vSphere Web Client oder dem `esxcli system syslog`-Befehl einzurichten und das Hostprofil zu speichern. Sie können Syslog auch über die Schnittstelle „Hostprofile“ einrichten.

Voraussetzungen

- Wenn Sie einen Remote-Syslog-Host verwenden möchten, richten Sie diesen Host ein, bevor Sie Hostprofile anpassen.
- Stellen Sie sicher, dass Sie auf einen vSphere Web Client zugreifen können, der eine Verbindung mit dem vCenter Server-System herstellen kann.

Vorgehensweise

1 Klicken Sie im vSphere Web Client auf **Regeln und Profile** und klicken Sie dann auf **Hostprofile**.

2 (Optional) Wenn kein Referenzhost in Ihrer Umgebung vorhanden ist, klicken Sie auf das Symbol **Hostprofil extrahieren**, um ein Hostprofil zu erstellen.

3 Klicken Sie mit der rechten Maustaste auf das zu ändernde Hostprofil und wählen Sie **Hostprofil bearbeiten**.

4 Lassen Sie den Namen und die Beschreibung unverändert und klicken Sie auf **Weiter**.

5 Klicken Sie auf **Erweiterte Konfigurationseinstellungen**, auf den Ordner **Erweiterte Optionen** und auf **Erweiterte Konfigurationsoptionen**.

  Sie können die Syslog-Einstellungen hier festlegen.

6 Wenn Sie einen ESXi 5.0-Host einrichten, der keinen vorher konfigurierten Syslog-Server hatte, müssen Sie eine erweiterte Konfigurationsoption erstellen.

   a Klicken Sie auf das Pluszeichen.

   b Klicken Sie auf die neue erweiterte Konfigurationsoption am Beginn der Optionsliste und wählen Sie **Feste Option konfigurieren** aus dem Dropdown-Menü.

   c Geben Sie Syslog.global.loghost als Option und Ihren Host als Wert an.

   Wenn Sie einen ESXi-Host Version 5.1 oder höher oder einen ESXi 5.0-Host konfigurieren, für den Syslog konfiguriert ist, befindet sich Syslog.global.loghost bereits in der Liste der erweiterten Optionen.

7 Klicken Sie auf **OK**, um die Hostprofileinstellungen zu speichern.

Weiter

- Erstellen Sie eine Regel, anhand der das Hostprofil für alle Hosts angewendet wird, die Sie mit den von Ihnen auf dem Referenzhost angegebenen Einstellungen bereitstellen möchten (siehe „Erstellen einer Regel und Zuweisen eines Hostprofils zu Hosts“, auf Seite 94).
- Bei Hosts, die bereits mit Auto Deploy bereitgestellt wurden, führen Sie die Übereinstimmungstests und die Reparaturvorgänge durch, um Sie mit dem neuen Image-Profil zu versehen. Weitere Informationen hierzu finden Sie unter „Testen und Reparieren der Regelübereinstimmung“, auf Seite 96.
- Schalten Sie nicht bereitgestellte Hosts ein, um sie mit dem neuen Image-Profil bereitzustellen.

Erstellen des Netzwerks für Ihren Auto Deploy-Host im vSphere Web Client

Sie können Ihr Netzwerk für Ihren Auto Deploy-Referenzhost einrichten und das Hostprofil für alle anderen Hosts übernehmen, um eine vollständig funktionale Netzwerkumgebung zu gewährleisten.

Voraussetzungen

Stellen Sie mithilfe von Auto Deploy den Host bereit, den Sie als Ihren Referenzhost mit einem ESXi-Image verwenden möchten.

Vorgehensweise

1 Wählen Sie im vSphere Web Client den Host aus und klicken Sie auf die Registerkarte **Netzwerk**.

2 Legen Sie die Netzwerkeinstellungen fest.

   Wenn Sie virtuelle Switches und keine vSphere Distributed Switches verwenden, fügen Sie keine anderen VMkernel-Netzwerkkarten zu vSwitch0 hinzu.

3 Wenn der Referenzhost konfiguriert ist, starten Sie das System neu, um sicherzustellen, dass vmk0 mit dem Verwaltungsnetzwerk verbunden ist.

4 Erstellen Sie ein Hostprofil aus dem Host.

Weiter

- Erstellen Sie eine Regel, durch die das Hostprofil auf alle Hosts angewendet wird, die Sie mit den von Ihnen auf dem Referenzhost angegebenen Einstellungen bereitstellen möchten. Weitere Informationen hierzu finden Sie unter „Erstellen einer Regel und Zuweisen eines Hostprofils zu Hosts“, auf Seite 94.
- Bei Hosts, die bereits mit Auto Deploy bereitgestellt wurden, führen Sie die Übereinstimmungstests und die Reparaturvorgänge durch, um sie mit dem neuen Hostprofil zu versehen. Weitere Informationen hierzu finden Sie unter „Testen und Reparieren der Regelübereinstimmung“, auf Seite 96.
- Schalten Sie nicht bereitgestellte Hosts ein, um sie mit dem Hostprofil bereitzustellen.

Berücksichtigen und Implementieren Ihrer Partitionierungsstrategie

Standardmäßig stellt Auto Deploy Hosts nur bereit, wenn eine Partition auf dem Host zur Verfügung steht. Sie können einen Referenzhost einrichten, um alle Hosts automatisch zu partitionieren, die mit Auto Deploy bereitgestellt werden.



VORSICHT Wenn Sie das Standardverhalten für die automatische Partitionierung ändern, überschreibt Auto Deploy bestehende Partitionen unabhängig vom Inhalt. Stellen Sie beim Aktivieren dieser Option sicher, dass es zu keinem unerwünschten Datenverlust kommt.

Sie müssen den Parameter **skipPartitioningSsds=TRUE** auf dem Referenzhost festlegen, damit lokale SSDs während der automatischen Partitionierung unpartitioniert bleiben.

Weitere Informationen zum Verhindern der SSD-Formatierung während der automatischen Partitionierung finden Sie in der *vSphere-Speicher*-Dokumentation.

Voraussetzungen

- Stellen Sie mithilfe von Auto Deploy den Host bereit, den Sie als Ihren Referenzhost mit einem ESXi-Image verwenden möchten.
- Stellen Sie sicher, dass Sie auf einen vSphere Web Client zugreifen können, der eine Verbindung mit dem vCenter Server-System herstellen kann.

Vorgehensweise

1 Wählen Sie im vSphere Web Client den Host aus, den Sie als Referenzhost verwenden möchten, und klicken Sie auf **Verwalten**.

2 Klicken Sie auf **Einstellungen**.

3 Klicken Sie auf **System**, um die Systemoptionen zu öffnen, und klicken Sie auf **Erweiterte Systemeinstellungen**.

4 Führen Sie einen Bildlauf zu `VMkernel.Boot.autoPartition` durch und legen Sie den Wert auf „True“ fest.

5 (Optional) Wenn lokale SSDs unpartitioniert bleiben sollen, führen Sie einen Bildlauf zu `VMkernel.Boot.skipPartitioningSsds` durch und legen Sie „True“ als Wert fest.

6 Falls noch nicht vorhanden, erstellen Sie ein Hostprofil für Ihren Referenzhost.

7 Schreiben Sie mit Auto Deploy PowerCLI eine Regel, mit der das Hostprofil Ihres Referenzhosts sofort beim Starten auf alle Hosts angewendet wird.

Die automatische Partitionierung wird beim Starten der Hosts durchgeführt.

Erweiterte Verwaltungsaufgaben

In den meisten Fällen verwalten Sie Ihre Auto Deploy-Umgebung, indem Sie die Systemeinrichtung vorbereiten, Regeln schreiben und Hosts bereitstellen. In einigen Fällen führen Sie möglicherweise erweiterte Verwaltungsaufgaben durch, wie z. B. das erneute Registrieren des Auto Deploy-Servers oder das Zuweisen einer statischen IP-Adresse zu jedem Host.

Einrichten von Hostprofilen für statische IP-Adressen im vSphere Web Client

Standardmäßig werden Hosts, die mit Auto Deploy bereitgestellt werden, von einem DHCP-Server DHCP-Adressen zugewiesen. Mit dem Auto Deploy-Hostanpassungsmechanismus können Sie den Hosts statische IP-Adressen zuweisen.

Voraussetzungen

- Richten Sie Ihre Auto Deploy-Umgebung ein.

- Starten Sie den Host unter Verwendung von Auto Deploy.
- Extrahieren Sie ein Hostprofil aus dem Host.

Vorgehensweise

1. Gehen Sie im vSphere Web Client zum vCenter Server, auf dem der Auto Deploy-Host verwaltet wird, wählen Sie **Richtlinien und Profile** und klicken Sie auf **Hostprofile**.
2. Klicken Sie mit der rechten Maustaste auf das extrahierte Hostprofil und wählen Sie **Einstellungen bearbeiten**.
3. Verwenden Sie den Standardwert für den Namen und die Beschreibung. Klicken Sie auf **Weiter**.
4. Ändern Sie die Standard-IP-Adresse, indem Sie auf **Netzwerkkonfiguration > Hostportgruppe > Verwaltungsnetzwerk > IP-Adresseinstellungen** klicken.
5. Wählen Sie im Dropdown-Menü **IPv4-Adresse** die Option **Vom Benutzer angegebene IP-Adresse, die beim Übernehmen der Konfiguration verwendet werden soll**.
6. Wenn sich der Host in einem anderen Subnetz als das vCenter Server-System befindet, wählen Sie **Netzwerkkonfiguration > NetStack-Instanz > defaultTcpipStack > DNS-Konfiguration** und geben im Textfeld **Standard-IPv4-Gateway** die Standardroute an.
7. Wählen Sie **Netzwerkkonfiguration > NetStack-Instanz > defaultTcpipStack > DNS-Konfiguration** aus.
8. Vergewissern Sie sich, dass das Kontrollkästchen **Flag, das angibt, ob DHCP verwendet werden soll** nicht aktiviert ist.
9. Klicken Sie mit der rechten Maustaste auf den Host und wählen Sie **Alle vCenter-Aktionen > Hostprofile > Hostprofil anhängen**.
10. Wählen Sie das Profil aus, das angehängt werden soll, und klicken Sie auf **Weiter**.
11. Geben Sie die IP-Adresse und die Netzmaske an und klicken Sie auf **Beenden**.
12. Starten Sie den ESXi-Host neu.

Die IP-Adresse wird als Hostanpassung gespeichert und auf den Host angewendet.

Hostanpassung im vSphere Web Client

Um Hosts mit gemeinsam genutzten Attributen anzupassen, können Sie ein Hostprofil in einem Referenzhost erstellen. Sie können zum Anpassen von einzelnen Hosts einige Felder im Hostprofil einrichten, dessen Werte der Benutzer für jeden Host eingeben muss.

Hostprofile ermöglichen es Ihnen, vorab Informationen anzugeben, z. B. die Einrichtung des Speichers oder des Syslogs in einem Referenzhost, und das Hostprofil auf einen Satz von Zielhosts anzuwenden, die die gleichen Einstellungen gemeinsam nutzen. Sie können auch Hostprofile verwenden, um anzugeben, dass bestimmte Einstellungen vom Host abhängig sind. Wenn Sie dies tun, wird der Host im Wartungsmodus gestartet, wenn Sie ihn mit Auto Deploy bereitstellen. Standardisieren Sie den Host oder setzen Sie die Anpassung des Hosts zurück, wenn Sie aufgefordert werden, eine Eingabe vorzunehmen. Das System speichert Ihre Eingaben und verwendet sie beim nächsten Start des Hosts.

HINWEIS Die Hostanpassung wird nicht an einem Speicherort oder in einem Format gespeichert, auf das Administratoren zugreifen können. Verwenden Sie die Benutzerschnittstelle „Hostprofile" des vSphere Web Client, um die Anpassung zu ändern.

Wenn der Hostprofil so eingestellt ist, dass der Benutzer zur Eingabe aufgefordert wird, müssen Sie einen Wert in das Dialogfeld eingeben, das beim Zurücksetzen der Hostanpassung erscheint. Wenn Sie keinen Wert eingeben, tritt ein Fehler auf.

Tabelle 4-9. Hostprofil-Optionen mit iSCSI-Abfrage

Informationen, für die der Benutzer zur Eingabe aufgefordert werden soll	Festlegen der Hostprofil-Option
Wenn Sie ein Hostprofil auf ein System anwenden, das auch ein Profil für iSCSI enthält, werden Sie aufgefordert, mehrere Eigenschaften einzugeben. Für viele der Eigenschaften steht ein Standard-Systemwert zur Verfügung. Für einige Eigenschaften müssen Sie einen Wert angeben, andernfalls tritt ein Fehler auf. **IQN-Name**: Wenn das iSCSI-Setup einen IQN-Namen verwendet, werden Sie aufgefordert, ihn einzugeben, wenn Sie das Hostprofil anwenden. Sie können erst dann fortfahren, wenn Sie den Namen eingegeben haben. **CHAP-Informationen**: Wenn Sie iSCSI so einrichten, dass eine CHAP-Authentifizierung erforderlich ist, werden Sie aufgefordert, die CHAP-Informationen einschließlich des Benutzernamens und des Schlüssels einzugeben, wenn Sie das Hostprofil anwenden. Sie können erst dann fortfahren, wenn Sie den Namen eingegeben haben.	1 Wählen Sie **Hostprofil bearbeiten**, klicken Sie auf **Speicherkonfiguration** und klicken Sie auf **Konfiguration des iSCSI-Initiators**. 2 Wählen Sie den Ordner für einen bereits aktivierten Initiator aus und richten Sie den Initiator ein. 3 Richten Sie den Initiator ein. Im Rahmen der Hostanpassung wird für viele Felder eine Eingabeaufforderung angezeigt.

Tabelle 4-10. Hostprofil-Optionen, die den Benutzer auffordern, eine Eingabe zum Speicher vorzunehmen

Informationen, für die der Benutzer zur Eingabe aufgefordert werden soll	Festlegen der Hostprofil-Option
Sie richten die feste PSP-Konfiguration ein und möchten den Benutzer auffordern, die Adapter- und Ziel-IDs für die Speicher-Arrays einzugeben, die die feste PSP-Konfiguration verwenden sollen.	Sie können die Option nur einrichten, wenn der Adapter zur Verwendung der festen PSP-Konfiguration eingerichtet wurde. 1 Wählen Sie **Hostprofil bearbeiten** und klicken Sie auf **Speicherkonfiguration**. 2 Klicken Sie auf **Native Multipathing (NMP)**. 3 Klicken Sie auf **Konfiguration der Pfadauswahlrichtlinie (PSP)**. 4 Wählen Sie im Fenster „Bevorzugter Pfad“ **Benutzer auffordern, Adapter und Ziel-IDs auf dem Host einzugeben** aus.
Konfigurieren Sie die FCoE-Adapter-Aktivierung basierend auf einer vom Benutzer angegebenen MAC-Adresse.	Sie können die Option nur einrichten, wenn ein Aktivierungsprofil vorhanden ist. 1 Wählen Sie **Hostprofil bearbeiten** und klicken Sie auf **Speicherkonfiguration**. 2 Klicken Sie auf **Software-FCoE-Konfiguration**. 3 Klicken Sie auf **Adapterkonfiguration**. 4 Klicken Sie auf das Aktivierungsprofil und klicken Sie auf **Profilrichtlinie**. 5 Wählen Sie **Aktivierungsrichtlinie auf Basis der MAC-Adresse des Adapters** aus dem Dropdown-Menü aus.

Tabelle 4-11. Hostprofil-Optionen mit Sicherheitsabfrage

Informationen, für die der Benutzer zur Eingabe aufgefordert werden soll	Festlegen der Hostprofil-Option
Administratorkennwort für ESXi-Host, wenn der Host zum ersten Mal gestartet wird.	1 Wählen Sie **Hostprofil bearbeiten** und klicken Sie auf **Sicherheit und Dienste**. 2 Klicken Sie auf **Sicherheitseinstellungen** und dann auf **Sicherheitskonfiguration**. 3 Wählen Sie im rechten Bereich **Vom Benutzer eingegebenes Kennwort zum Konfigurieren des Administratorkennworts** aus dem Dropdown-Menü **Administratorkennwort** aus.
Konfiguriert einen Benutzer für den ESXi-Host vor, fordert den Benutzer jedoch zur Eingabe des Kennworts für diesen Benutzer auf jedem Host auf, wenn der Host zum ersten Mal gestartet wird.	Sie können diese Aufgabe nur ausführen, wenn die Benutzerkonfiguration bereits vorhanden ist. Konfigurieren Sie den Benutzer, indem Sie eine der Optionen auswählen. ■ Die Option **Feste Benutzerkonfigurationen zuweisen** steht aus Gründen der Kompatibilität mit ESX/ESXi 4.1-Systemen zur Verfügung. Bei dieser Option wird das Kennwort im Klartext angezeigt. ■ Die Option **Erweiterte feste Benutzerkonfigurationen zuweisen** ist für Benutzer von ESXi 5.0-Systemen (und höher) vorgesehen. ■ **Benutzerkonfiguration im Profil angeben, aber während der Hostkonfiguration Kennwort abfragen** ermöglicht Ihnen das Festlegen von Angaben zum Benutzer, fragt jedoch auf jedem Host ein Kennwort ab.
Fordern Sie den Benutzer auf, seine Anmeldeinformationen einzugeben, wenn der Host der Active Directory-Domäne beitritt.	1 Stellen Sie das Profil für die Authentifizierungskonfiguration so ein, dass eine feste Domäne verwendet wird. a Wählen Sie **Hostprofil bearbeiten** und klicken Sie auf **Sicherheit und Dienste**. b Klicken Sie auf **Sicherheitseinstellungen** und dann auf **Authentifizierungskonfiguration**. c Klicken Sie auf **Active Directory-Konfiguration**. d Wählen Sie aus dem Dropdown-Menü „Domänenname“ die Option **Festen Domänennamen konfigurieren** aus. 2 Richten Sie die Methode für den Domänenbeitritt so ein, dass eine Meldung angezeigt wird. a Wählen Sie **Hostprofil bearbeiten**, klicken Sie auf **Sicherheit und Dienste** und klicken Sie auf **Authentifizierungskonfiguration**. b Klicken Sie auf **Active Directory-Konfiguration**. c Wählen Sie aus dem Dropdown-Menü für die Methode „Domäne beitreten“ die Option **Vom Benutzer angegebene AD-Anmeldedaten beim Beitreten der Domäne verwenden** aus.

Tabelle 4-12. Hostprofil-Optionen mit Netzwerkabfrage

Informationen, für die der Benutzer zur Eingabe aufgefordert werden soll	Festlegen der Hostprofil-Option
Fordern Sie den Benutzer zur Eingabe der MAC-Adresse für eine Portgruppe auf. Sie können veranlassen, dass das System den Benutzer in allen Fällen (vom Benutzer angegebene MAC-Adresse...) oder nur dann auffordert, wenn keine Standardadresse verfügbar ist.	1 Wählen Sie **Hostprofil bearbeiten**, klicken Sie auf **Netzwerkkonfiguration** und klicken Sie auf **Hostportgruppe**. 2 Klicken Sie auf **Verwaltungsnetzwerk**. 3 Wählen Sie im Feld **Festlegen, wie die MAC-Adresse für vmknic entschieden werden soll** aus, wie das System die MAC-Adressen verwalten soll. ■ **Vom Benutzer angegebene MAC-Adresse, die beim Übernehmen der Konfiguration verwendet werden soll** ■ **Benutzer zur Eingabe der MAC-Adresse auffordern, falls keine Standardadresse verfügbar ist**
Fordern Sie den Benutzer auf, die IPv4-Adresse für jeden ESXi-Host einzugeben, auf den das Profil angewendet wird. Sie können veranlassen, dass das System den Benutzer in allen Fällen (vom Benutzer angegebene IPv4-Adresse...) oder nur dann auffordert, wenn keine Standardeinstellung verfügbar ist.	1 Wählen Sie **Hostprofil bearbeiten**, klicken Sie auf **Netzwerkkonfiguration** und klicken Sie auf **Hostportgruppe**. 2 Klicken Sie auf **Verwaltungsnetzwerk** und klicken Sie auf **IP-Adresseinstellungen**. 3 Wählen Sie im Feld **IPv4-Adresse** aus, wie das System die IPv4-Adresse verwalten soll. ■ **Vom Benutzer angegebene IPv4-Adresse, die beim Übernehmen der Konfiguration verwendet werden soll** ■ **Benutzer zur Eingabe der IPv4-Adresse auffordern, falls keine Standardadresse verfügbar ist**
Fordern Sie den Benutzer auf, die IPv6-Adresse für jeden ESXi-Host einzugeben, auf den das Profil angewendet wird. Sie können veranlassen, dass das System den Benutzer in allen Fällen (vom Benutzer angegebene IPv6-Adresse...) oder nur dann auffordert, wenn keine Standardeinstellung verfügbar ist.	1 Wählen Sie **Hostprofil bearbeiten**, klicken Sie auf **Netzwerkkonfiguration** und klicken Sie auf **Hostportgruppe**. 2 Klicken Sie auf **Verwaltungsnetzwerk** und klicken Sie auf **IP-Adresseinstellungen**. 3 Wählen Sie im Feld **Statische IPv6-Adresse** aus, wie das System die IPv6-Adresse verwalten soll. ■ **Vom Benutzer angegebene IPv6-Adresse, die beim Übernehmen der Konfiguration verwendet werden soll** ■ **Benutzer zur Eingabe der manuellen IPv6-Adresse auffordern, falls keine Standardadresse verfügbar ist**
Fordern Sie den Benutzer zur Eingabe des DNS-Namens des Hosts auf. Sie können veranlassen, dass das System den Benutzer in allen Fällen (vom Benutzer angegebener Hostname...) oder nur dann auffordert, wenn keine Standardeinstellung verfügbar ist.	1 Wählen Sie **Hostprofil bearbeiten**, klicken Sie auf **Netzwerkkonfiguration** und klicken Sie auf **DNS-Konfiguration**. 2 Wählen Sie im Feld „Hostname“ aus, wie das System die DNS-Konfiguration verwalten soll. ■ **Benutzer zur Eingabe des Hostnamens auffordern, falls kein Standardname verfügbar ist** ■ **Vom Benutzer angegebener Hostname, der beim Übernehmen der Konfiguration verwendet werden soll**

Tabelle 4-12. Hostprofil-Optionen mit Netzwerkabfrage (Fortsetzung)

Informationen, für die der Benutzer zur Eingabe aufgefordert werden soll	Festlegen der Hostprofil-Option
Fordern Sie den Benutzer zur Eingabe der MAC-Adresse für einen Distributed Switch, dessen Portgruppe oder einen seiner Dienste auf. Klicken Sie mit der rechten Maustaste auf das Symbol des Ordners der virtuellen Netzwerkkarte des Hosts und klicken Sie auf das Symbol **Unterprofil hinzufügen**, um die Komponente zu ermitteln, auf die diese Einstellung angewendet wird. Sie können entscheiden, ob Sie den Benutzer zur Eingabe nur dann auffordern, wenn kein Standardwert verfügbar ist, oder in allen Fällen.	1 Öffnen Sie **Netzwerkkonfiguration**. 2 Klicken Sie auf **Virtuelle Netzwerkkarte des Hosts**. 3 Wählen Sie im Feld **Festlegen, wie die MAC-Adresse für vmknic entschieden werden soll** aus, wie das System die MAC-Adresse für den Distributed Switch verwalten soll. ■ **Vom Benutzer angegebene MAC-Adresse, die beim Übernehmen der Konfiguration verwendet werden soll** ■ **Benutzer zur Eingabe der MAC-Adresse auffordern, falls keine Standardadresse verfügbar ist**
Fordern Sie den Benutzer zur Eingabe der IPv4-Adresse für einen Distributed Switch, dessen Portgruppe oder einen seiner Dienste auf. Klicken Sie mit der rechten Maustaste auf das Symbol des Ordners der virtuellen Netzwerkkarte des Hosts und klicken Sie auf das Symbol **Unterprofil hinzufügen**, um die Komponente zu ermitteln, auf die diese Einstellung angewendet wird. Sie können entscheiden, ob Sie den Benutzer zur Eingabe nur dann auffordern, wenn kein Standardwert verfügbar ist, oder in allen Fällen.	1 Öffnen Sie **Netzwerkkonfiguration**. 2 Klicken Sie auf **Virtuelle Netzwerkkarte des Hosts**. 3 Klicken Sie auf **IP-Adresseinstellungen**. 4 Wählen Sie im Feld „IPv4-Adresse“ aus, wie das System die IPv4-Adresse für den Distributed Switch handhaben soll. ■ **Vom Benutzer angegebene IPv4-Adresse, die beim Übernehmen der Konfiguration verwendet werden soll** ■ **Benutzer zur Eingabe der IPv4-Adresse auffordern, falls keine Standardadresse verfügbar ist**
Fordern Sie den Benutzer zur Eingabe der IPv6-Adresse für einen Distributed Switch, dessen Portgruppe oder einen seiner Dienste auf. Klicken Sie mit der rechten Maustaste auf das Symbol des Ordners der virtuellen Netzwerkkarte des Hosts und klicken Sie auf das Symbol **Unterprofil hinzufügen**, um die Komponente zu ermitteln, auf die diese Einstellung angewendet wird. Sie können entscheiden, ob Sie den Benutzer zur Eingabe nur dann auffordern, wenn kein Standardwert verfügbar ist, oder in allen Fällen.	1 Öffnen Sie **Netzwerkkonfiguration**. 2 Öffnen Sie **Virtuelle Netzwerkkarte des Hosts**. 3 Öffnen Sie **IP-Adresseinstellungen**. 4 Wählen Sie im Feld **Statische IPv6-Adresse** aus, wie das System die IPv6-Adressen für den Distributed Switch verwalten soll. ■ **Vom Benutzer angegebene IPv6-Adresse, die beim Übernehmen der Konfiguration verwendet werden soll** ■ **Benutzer zur Eingabe der IPv6-Adresse auffordern, falls keine Standardadresse verfügbar ist**

Best Practices und Sicherheitsempfehlungen für Auto Deploy

Gehen Sie bei der Installation von vSphere Auto Deploy und der Verwendung von Auto Deploy mit anderen vSphere-Komponenten den Best Practices entsprechend vor. Richten Sie eine hochverfügbare Auto Deploy-Infrastruktur in großen Produktionsumgebungen oder bei der Verwendung des statusfreien Cachings ein. Befolgen Sie dieselben Sicherheitsrichtlinien wie in einer PXE-Start-Umgebung und berücksichtigen Sie die Empfehlungen in diesem Kapitel.

Best Practices für Auto Deploy

Sie können die verschiedenen empfohlenen Vorgehensweisen für Auto Deploy befolgen, vSphere HA konfigurieren und Ihre Umgebung anderweitig für Auto Deploy optimieren.

Weitere Informationen zu empfohlenen Vorgehensweisen (sogenannten „Best Practices“) finden Sie in der VMware-Knowledgebase.

Best Practices für Auto Deploy und vSphere HA

Anhand der empfohlenen Vorgehensweisen können Sie die Verfügbarkeit der virtuelle Maschinen auf Hosts verbessern, die mit Auto Deploy bereitgestellt wurden.

In manchen Umgebungen werden die mit Auto Deploy bereitgestellten Hosts mit einem Distributed Switch konfiguriert oder die virtuelle Maschinen, die auf diesen Hosts ausgeführt werden, werden mit Auto Start Manager konfiguriert. Stellen Sie das vCenter Server-System in Umgebungen dieser Art so bereit, dass seine Verfügbarkeit mit der Verfügbarkeit des Auto Deploy-Servers übereinstimmt. Es sind mehrere Ansätze denkbar.

- Stellen Sie in einer Machbarkeitsnachweis-Umgebung das vCenter Server-System und den Auto Deploy-Server auf demselben System bereit. In allen anderen Situationen sollten Sie zwei Server auf getrennten Systemen installieren.
- Stellen Sie das vCenter Server-System in einer virtuellen Maschine bereit. Führen Sie die virtuelle Maschine von vCenter Server in einem vSphere HA-aktivierten Cluster aus und konfigurieren Sie die virtuelle Maschine mit der vSphere HA-Neustartpriorität „Hoch". Nehmen Sie zwei oder mehrere Hosts, die nicht von Auto Deploy verwaltet werden, in den Cluster auf und verknüpfen Sie mithilfe einer Regel (VM-zu-Host-Regel: vSphere HA DRS erforderlich) die virtuelle vCenter Server-Maschine mit diesen Hosts. Sie können die Regel einrichten und anschließend DRS deaktivieren, wenn Sie DRS nicht im Cluster verwenden möchten. Je mehr Hosts es gibt, die nicht von Auto Deploy verwaltet werden, desto widerstandsfähiger ist die Umgebung gegenüber Hostausfällen.

  HINWEIS Dieser Ansatz ist nicht geeignet, wenn Sie Auto Start Manager verwenden. Auto Start Manager wird in einem Cluster nicht unterstützt, der für vSphere HA aktiviert ist.

Best Practices für Netzwerke mit Auto Deploy

Vermeiden Sie Netzwerkprobleme, indem Sie die empfohlenen Vorgehensweisen für Netzwerke von Auto Deploy befolgen.

Auto Deploy und IPv6
Da Auto Deploy die iPXE-Infrastruktur nutzt, ist für jeden Host eine IPv4-Adresse erforderlich. Nach der Bereitstellung können Sie die Hosts für die Verwendung von IPv6 manuell neu konfigurieren und dem vCenter Server über IPv6 hinzufügen. Beim Neustart eines statusfreien Hosts geht die IPv6-Konfiguration allerdings verloren.

Zuweisung der IP-Adresse
Verwenden Sie DHCP-Reservierungen für die Zuteilung von Adressen. Feste IP-Adressen werden vom Hostanpassungsmechanismus unterstützt, aber das Eingeben der Daten für jeden Host ist nicht empfehlenswert.

VLAN-Überlegungen
Verwenden Sie Auto Deploy in Umgebungen ohne VLANs.

Wenn Sie Auto Deploy in einer Umgebung mit VLANs einsetzen möchten, müssen Sie sicherstellen, dass die Hosts, die Sie bereitstellen möchten, auf den DHCP-Server zugreifen können. Die Art, wie einem VLAN die Hosts zugewiesen sind, hängt von der Konfiguration Ihrer Site ab. Die VLAN-ID wird möglicherweise vom Switch oder Router zugewiesen oder im Host-BIOS oder Hostprofil festgelegt. Fragen Sie Ihren Netzwerkadministrator nach den Schritten, die durchzuführen sind, damit die Hosts auf den DHCP-Server zugreifen können.

Best Practices für Auto Deploy und VMware Tools

Wenn Sie Hosts mit Auto Deploy bereitstellen, können Sie ein Image-Profil auswählen, das VMware Tools umfasst, oder wählen Sie ein kleineres, dem Image-Profil zugeordnetes Image ohne VMware Tools aus.

Sie können zwei Image-Profile von der VMware-Downloadsite herunterladen.

- `xxxxx-standard`: Ein Image-Profil, das die VMware Tools-Binärdateien umfasst und für das auf einer virtuellen Maschine ausgeführte Gastbetriebssystem erforderlich ist. Das Image hat in der Regel den Namen esxi-*version*-*xxxxx*-standard.

- `xxxxx-no-tools`: Ein Image-Profil, das die VMware Tools-Binärdateien nicht enthält. Dieses Image-Profil ist in der Regel kleiner, hat weniger Arbeitsspeicher-Overhead und startet in einer PXE-Boot-Umgebung schneller. Das Image hat in der Regel den Namen esxi-*version*-*xxxxx*-no-tools.

Ab vSphere 5.0 Update 1 können Sie ESXi mit jedem dieser Image-Profile bereitstellen.

- Wenn die Netzwerkstartzeit keine Rolle spielt und Ihre Umgebung genügend freien Speicherplatz und Arbeitsspeicher-Overhead aufweist, sollten Sie das Image verwenden, in dem VMware Tools enthalten ist.
- Wenn die Netzwerkstartzeit mit dem Standard-Image zu langsam ist oder Sie Speicherplatz auf den Hosts sparen möchten, können Sie stattdessen das Image-Profil ohne VMware Tools verwenden und die Binärdateien für VMware Tools im freigegebenen Speicher ablegen. Weitere Informationen finden Sie unter „Bereitstellen eines ESXi-Hosts mithilfe eines Image-Profils ohne VMware Tools“, auf Seite 128.

Arbeitslastverwaltung mit Auto Deploy – Empfohlene Vorgehensweisen

Das gleichzeitige Starten einer großen Anzahl von Hosts stellt eine erhebliche Last für den Auto Deploy-Server dar. Da Auto Deploy im Kern ein Webserver ist, können Sie vorhandene Webserver-Skalierungstechnologien verwenden, um die Last zu verteilen. Beispielsweise kann ein bzw. können mehrere Caching-Reverse-Proxy-Server mit Auto Deploy verwendet werden. Die Reverse-Proxys stellen die statischen Dateien bereit, die den größten Teil eines ESXi-Start-Images ausmachen. Konfigurieren Sie den Reverse-Proxy, um statische Inhalte zwischenzuspeichern und alle Anforderungen über den Auto Deploy-Server weiterzuleiten. Weitere Informationen erhalten Sie im Video „Verwenden von Reverse-Web-Proxyservern für die Skalierbarkeit von Auto Deploy“.



Verwenden von Reverse-Web-Proxyservern für die Skalierbarkeit von Auto Deploy (http://link.brightcove.com/services/player/bcpid2296383276001?bctid=ref:video_reverse_web_proxy_for_auto_deploy_scalability)

Nutzen Sie mehrere TFTP-Server, um auf verschiedene Proxyserver zu verweisen. Verwenden Sie einen TFTP-Server für jeden Reverseproxyserver. Richten Sie den DHCP-Server anschließend so ein, dass er verschiedene Hosts an verschiedene TFTP-Server sendet.

Wenn Sie die Hosts starten, werden sie vom DHCP-Server an verschiedene TFTP-Server weitergeleitet. Jeder TFTP-Server leitet die Hosts an einen anderen Server weiter, und zwar entweder an den Auto Deploy-Server oder an einen Reverseproxyserver. Dadurch wird die Last auf dem Auto Deploy-Server signifikant reduziert.

Nach einem massiven Stromausfall sollten Sie die Hosts Cluster um Cluster nacheinander hochfahren. Wenn Sie mehrere Cluster gleichzeitig online bringen, treten möglicherweise CPU-Engpässe beim Auto Deploy-Server ein. Bis alle Hosts hochgefahren sind, kann es eine Weile dauern. Der Engpass fällt weniger heftig aus, wenn Sie den Reverse-Proxy einrichten.

Best Practices für die vSphere Auto Deploy-Protokollierung und Fehlerbehebung

Zum Beheben von Problemen, die bei vSphere Auto Deploy auftreten, stehen Ihnen die Auto Deploy-Protokolldaten im vSphere Web Client zur Verfügung. Richten Sie Ihre Umgebung so ein, dass Protokolldaten und Core-Dumps an Remotehosts gesendet werden.

Auto Deploy-Protokolle
Laden Sie die Auto Deploy-Protokolle von der Auto Deploy-Seite im vSphere Web Client herunter. Weitere Informationen finden Sie unter „Herunterladen von Auto Deploy-Protokollen“, auf Seite 128.

Einrichten von Syslog
Richten Sie einen Remote-Syslog-Server ein. Weitere Informationen zur Konfiguration eines Syslog-Servers finden Sie in der Dokumentation zu *vCenter Server und Hostverwaltung*. Konfigurieren Sie den ersten Host, den Sie zum Verwenden des Remote-Syslog-Servers starten, und wenden Sie das Hostprofil dieses Hosts auf alle anderen Zielhosts an. Optional können Sie das

vCenter Server-Dienstprogramm vSphere Syslog Collector installieren und verwenden, das eine einheitliche Architektur für die Systemprotokollierung bietet sowie die Netzwerkprotokollierung und das Kombinieren von Protokollen mehrerer Hosts ermöglicht.

Einrichten von ESXi Dump Collector

Hosts, die mit Auto Deploy bereitgestellt wurden, verfügen über keine lokale Festplatte zum Speichern von Core-Dumps. Installieren Sie ESXi Dump Collector und richten Sie Ihren ersten Host so ein, dass alle Core-Dumps auf ESXi Dump Collector verwiesen werden. Wenden Sie anschließend das Hostprofil von diesem Host auf alle anderen Hosts an. Siehe „Konfigurieren des ESXi Dump Collectors mit ESXCLI“, auf Seite 112.

Verwenden von Auto Deploy in einer Produktionsumgebung

Wenn Sie von einem Machbarkeitsnachweis-Setup auf eine Produktionsumgebung umstellen, sorgen Sie dafür, dass die Umgebung widerstandsfähig wird.

- Schützen Sie den Auto Deploy-Server. Siehe „Best Practices für Auto Deploy und vSphere HA“, auf Seite 122.
- Schützen Sie alle anderen Server in Ihrer Umgebung, einschließlich des DHCP-Servers und des TFTP-Servers.
- Befolgen Sie die VMware-Sicherheitsrichtlinien, einschließlich der Richtlinien, die unter „Auto Deploy-Sicherheitsüberlegungen“, auf Seite 126 aufgeführt sind.

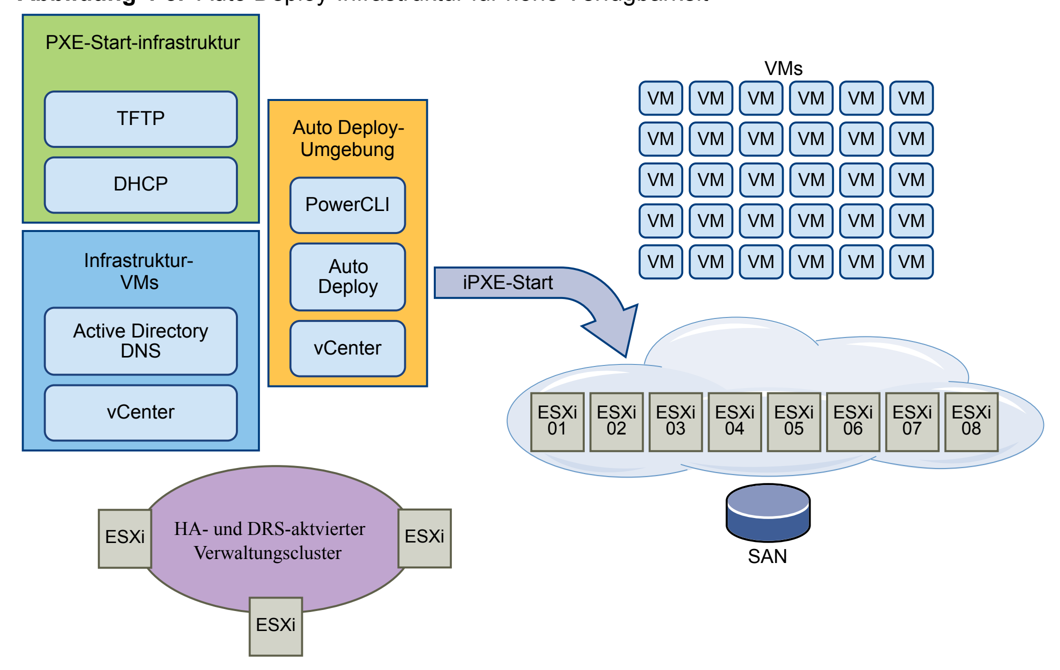
Einrichten einer hochverfügbaren Auto Deploy-Infrastruktur

In vielen Produktionssituationen ist eine hochverfügbare Auto Deploy-Infrastruktur erforderlich, um Datenverlust zu verhindern. Eine solche Infrastruktur ist zudem Voraussetzung zur Verwendung von Auto Deploy mit statusfreiem Caching.



Auto Deploy-Infrastruktur für hohe Verfügbarkeit (http://link.brightcove.com/services/player/bcpid2296383276001?bctid=ref:video_ha_auto_deploy_infrastructure)

Abbildung 4-5. Auto Deploy-Infrastruktur für hohe Verfügbarkeit



Voraussetzungen

Installieren Sie für den Verwaltungscluster ESXi auf drei Hosts. Stellen Sie die Verwaltungs-Cluster-Hosts nicht mit Auto Deploy bereit.

Sehen Sie sich das Video zur hochverfügbaren Auto Deploy-Infrastruktur an, um Information zu deren Implementierung zu erhalten:

Vorgehensweise

1 Aktivieren Sie vSphere HA und vSphere DRS auf dem Verwaltungs-Cluster.

2 Richten Sie die folgenden virtuellen Maschinen auf dem Verwaltungs-Cluster ein.

Infrastrukturkomponente	Beschreibung
Infrastruktur des PXE-Startvorgangs	TFTP- und DHCP-Server.
Infrastruktur-VM	Active Directory, DNS, vCenter Server
Auto Deploy-Umgebung	PowerCLI, Auto Deploy-Server, vCenter Server. Richten Sie diese Umgebung in Produktionssystemen auf einer einzelnen virtuellen Maschine oder auf drei separaten virtuellen Maschinen ein.

Der vCenter Server auf der virtuellen Maschine der Infrastruktur unterscheidet sich vom vCenter Server in der Auto Deploy-Umgebung.

3 Richten Sie Auto Deploy ein, um bei Bedarf weitere Hosts bereitzustellen.

Da die Komponenten auf dem Verwaltungs-Cluster mit vSphere HA geschützt sind, wird High Availability unterstützt.

Auto Deploy-Sicherheitsüberlegungen

Sie können Ihre Umgebung sicherer einrichten, wenn Sie mit den potenziellen Sicherheitsrisiken vertraut sind.

Sichern Sie Ihr Netzwerk wie bei jeder anderen PXE-basierten Bereitstellungsmethode. Auto Deploy überträgt Daten über SSL, um gelegentliche Störungen und Webspionage zu verhindern Allerdings wird die Authentizität des Clients oder des Auto Deploy-Servers während des Startens per PXE-Startvorgang nicht überprüft.

Das Start-Image, das der Auto Deploy-Server auf eine Maschine herunterlädt, kann über die folgenden Komponenten verfügen.

- Das Start-Image enthält immer die VIB-Pakete, aus denen das Image-Profil besteht.
- Das Hostprofil und die Hostanpasung sind im Start-Image enthalten, wenn Auto Deploy-Regeln so eingerichtet sind, dass der Host mit einem Hostprofil- oder einer Hostanpassungseinstellung bereitgestellt wird.
  - Das Administratorkennwort (root) und die Benutzerkennwörter, die im Hostprofil und in der Hostanpassung enthalten sind, sind mit MD5 verschlüsselt.
  - Alle anderen Kennwörter in Verbindung mit Profilen sind unverschlüsselt. Wenn Sie Active Directory mithilfe von Hostprofilen einrichten, werden die Kennwörter nicht geschützt.

    Verwenden Sie den vSphere-Authentifizierungsdienst zum Einrichten von Active Directory, um zu verhindern, dass die Active Directory-Kennwörter freigelegt werden.
- Die öffentlichen und privaten SSL-Schlüssel und das Zertifikat des Hosts sind im Start-Image enthalten.

Sie können das Sicherheitsrisiko von Auto Deploy erheblich reduzieren, indem Sie das Netzwerk, in dem Auto Deploy eingesetzt wird, vollständig isolieren.

Verwenden des Hostprofils „Konfiguration des Gerätealias“

In vSphere 5.5 und höher können Sie ein Gerät (Busadresse) dauerhaft einem Gerätenamen (Alias) zuweisen. Sie können die Zuordnung ändern, indem Sie das Hostprofil „Konfiguration des Gerätealias“ verwenden. Durch die dauerhafte Zuordnung können Warnungen beim Überprüfen der Übereinstimmung für statuslose Hosts vermieden werden, und sie ist auch für statusorientierte Hosts nützlich.

Das Hostprofil „Konfiguration des Gerätealias“ ist standardmäßig ausgewählt. Das bedeutet, das jedem Gerät Aliase zugewiesen werden. Wenn beispielsweise ein Host eine der Netzwerkkarten während des Startvorgangs nicht erkennt, ändern sich die Netzwerkkartenaliase nicht mehr. Das kann zur Verwaltung mit Skripts beitragen und in Fällen, in denen Sie ein Hostprofil eines Referenzhosts anwenden.

HINWEIS Um Fehler zu vermeiden, sollten Sie das Hostprofil „Konfiguration des Gerätealias“ nicht deaktivieren oder bearbeiten.

Um eine einheitliche, dauerhafte und stabile Gerätebenennung auf allen Hosts sicherzustellen, verwenden Sie das Gerätealias-Profil nur bei homogenen Hosts. Im Idealfall verfügen diese Hosts über identische Konfigurationen mit den gleichen Netzwerk- und Speicherkarten im PCI-Bus.

HINWEIS Achten Sie darauf, dass Sie stets über die neueste BIOS-Ebene verfügen. Bei Systemen mit früheren BIOS-Versionen stellt das BIOS möglicherweise keine genauen Angaben zum Ort der On-Board-Geräte bereit. ESXi wendet für diesen Fall Heuristik an, um den Alias auch für diese Geräte stabil zu halten. Dies funktioniert möglicherweise nicht immer, z. B. wenn Änderungen an der BIOS-Einstellung vorgenommen werden oder Geräte ausfallen.

Fehler bei der Übereinstimmung mit „Konfiguration des Gerätealias“

Wenn Hosts nicht vollständig homogen sind, also z. B. verschiedene PCI-Karten oder BIOS-Ebenen aufweisen, und Sie das Hostprofil eines Referenzhosts anwenden, kann eine Überprüfung der Übereinstimmung einen Fehler ergeben. Bei der Übereinstimmungsprüfung werden zusätzliche Geräte auf dem Host ignoriert, die sich nicht auf dem Referenzhost befanden. Wählen Sie den Host, der am wenigsten Geräte hat, als Referenzhost.

Wenn die Übereinstimmungsprüfung zeigt, dass die Hosts nicht vollständig homogen sind, können Übereinstimmungsfehler nicht ohne Änderung der Hardware selbst behoben werden.

Wenn die Übereinstimmungsprüfung Geräte erkennt, deren Aliase (z. B. Namen wie vmhba3) vom Referenzhost abweichen, kann eine Behebung möglich sein.

- Um den Fehler eines Hosts zu beheben, der nicht mit Auto Deploy bereitgestellt wird, führen Sie die Hostprofil-Fehlerbehebung durch und starten Sie den Host neu.
- Um einen Fehler eines Hosts zu beheben, der mit Auto Deploy bereitgestellt wird, stellen Sie den Host erneut bereit.

Upgrade von Systemen für Gerätealias-Profile

In ESXi-Versionen vor 5.5 ist das Profil „Konfiguration des Gerätealias“ nicht vorhanden. Beachten Sie bei einem Upgrade von älteren ESXi-Versionen auf ESXi 5.5 die folgenden Probleme:

- Bei installierten Hosts, die nicht mit Auto Deploy bereitgestellt wurden, werden die Aliase bei einem Upgrade des ESXi-Hosts beibehalten. Nach dem Upgrade bleiben die Aliase stabil, solange das BIOS die Informationen zur Verfügung stellt.

- Wenn Sie ein Upgrade für einen Cluster von ESXi-Hosts durchführen, die mit dem Auto Deploy-Image bereitgestellt wurden, ändern sich die Aliase nicht, da ESXi 5.5 den gleichen Algorithmus zum Generieren von Aliasen wie frühere Versionen verwendet. Generieren Sie ein neues Hostprofil für den Referenzhost. Dieses Hostprofil umfasst das Profil „Konfiguration des Gerätealias“. Richten Sie Auto Deploy ein, um das Hostprofil des Referenzhosts auf alle anderen Hosts anzuwenden und eine einheitliche Gerätebenennung im ganzen Cluster sicherzustellen.
- Beim Upgrade eines Systems sollte kein BIOS-Flash durchgeführt werden, da dadurch Aliase geändert werden können. Ein BIOS-Flash auf die neueste Ebene ist für Neuinstallationen besser geeignet.

Bereitstellen eines ESXi -Hosts mithilfe eines Image-Profils ohne VMware Tools

Wenn Sie ESXi-Hosts mit Auto Deploy bereitstellen, können Sie festlegen, dass die Bereitstellung mithilfe des Image-Profils erfolgt, das keine VMware Tools-Binärdateien enthält. Dieses Image-Profil ist in der Regel kleiner, hat einen niedrigeren Arbeitsspeicher-Overhead und startet in einer PXE-boot-Umgebung schneller.

Wenn die Netzwerkstartzeit mit dem Standard-Image zu langsam ist oder wenn Sie Speicherplatz auf den Hosts sparen möchten, können Sie das Image-Profil ohne VMware Tools verwenden und die Binärdateien von VMware Tools in einem freigegebenen Speicher ablegen.

Voraussetzungen

Laden Sie das Image-Profil „`xxxxx-no-tools`“ von der VMware-Downloadsite herunter.

Vorgehensweise

1. Starten Sie einen ESXi-Host, der nicht mit Auto Deploy bereitgestellt wurde.
2. Kopieren Sie das Verzeichnis `/productLocker` vom ESXi-Host in einen freigegebenen Speicher.
3. Ändern Sie die Variable *UserVars.ProductLockerLocation*, sodass sie auf das Verzeichnis `/productLocker` verweist.
   a. Wählen Sie im vSphere Web Client den Referenzhost aus und klicken Sie auf die Registerkarte **Verwalten**.
   b. Wählen Sie **Einstellungen** aus und klicken Sie auf **Erweiterte Systemeinstellungen**.
   c. Filtern Sie die Einstellungen nach **`uservars`** und wählen Sie **UserVars.ProductLockerLocation** aus.
   d. Klicken Sie auf das **Stift**-Symbol und bearbeiten Sie den Speicherort, damit er auf den freigegebenen Speicher verweist.
4. Erstellen Sie ein Hostprofil vom Referenzhost aus.
5. Erstellen Sie eine Auto Deploy-Regel, die das Image-Profil `xxxxx-no-tools` und das Hostprofil vom Referenzhost allen anderen Hosts zuweist.
6. Starten Sie die Zielhosts mit der Regel, sodass sie den Produkt-Locker-Speicherort vom Referenzhost übernehmen.

Herunterladen von Auto Deploy-Protokollen

Verwenden Sie zum Beheben von Problemen mit vSphere Auto Deploy die Auto Deploy-Protokolldaten im vSphere Web Client.

Voraussetzungen

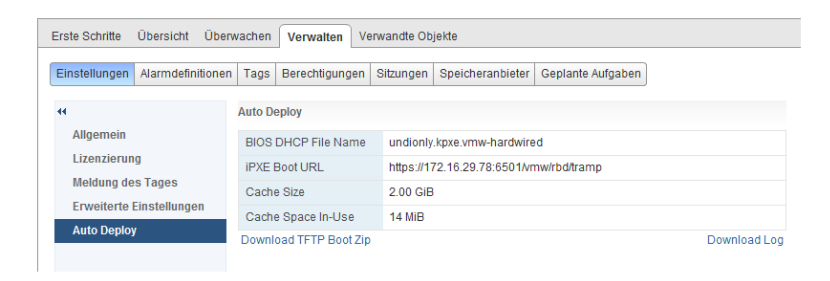
Verwenden Sie den vSphere Web Client, um sich bei der vCenter Server-Instanz anzumelden, bei der Auto Deploy registriert ist.

Vorgehensweise

1. Wählen Sie **vCenter-Bestandslisten** und anschließend das vCenter Server-System.

2 Klicken Sie auf der Registerkarte **Verwalten** auf **Einstellungen** und anschließend auf **Auto Deploy**.

3 Klicken Sie auf **Protokoll herunterladen**, um die Protokolldateien herunterzuladen.



Fehlerbehebung bei Auto Deploy

In den Themen zur Fehlerbehebung bei Auto Deploy finden Sie Lösungen für Situationen, in denen die Bereitstellung von Hosts mit Auto Deploy nicht erwartungsgemäß funktioniert.

Auto Deploy-TFTP-Zeitüberschreitungsfehler beim Start

Eine TFTP-Zeitüberschreitungs-Fehlermeldung erscheint, wenn ein von Auto Deploy bereitgestellter Host gestartet wird. Der Text der Meldung hängt vom BIOS ab.

Problem

Eine TFTP-Zeitüberschreitungs-Fehlermeldung erscheint, wenn ein von Auto Deploy bereitgestellter Host gestartet wird. Der Text der Meldung hängt vom BIOS ab.

Ursache

Der TFTP-Server ist ausgefallen oder nicht erreichbar.

Lösung

◆ Stellen Sie sicher, dass der TFTP-Dienst ausgeführt wird und von dem Host aus, den Sie zu starten versuchen, erreichbar ist.

Der Auto Deploy-Host wird mit der falschen Konfiguration gestartet

Ein Host wird mit einem anderen ESXi-Image, Hostprofil oder Ordnerspeicherort als in den Regeln angegeben gestartet.

Problem

Ein Host wird mit einem anderen ESXi-Image-Profil oder einer anderen Konfiguration als dem in den Regeln angegebenen Image-Profil bzw. der angegebenen Konfiguration gestartet. Beispiel: Sie ändern die Regeln, um ein anderes Image-Profil zuzuweisen, aber der Host verwendet nach wie vor das alte Image-Profil.

Ursache

Nachdem der Host zum vCenter Server-System hinzugefügt wurde, wird die Startkonfiguration vom vCenter Server-System festgelegt. Das vCenter Server-System ordnet dem Host ein Image-Profil, ein Hostprofil oder einen Ordnerspeicherort zu.

Lösung

◆ Verwenden Sie die PowerCLI-cmdlets `Test-DeployRuleSetCompliance` und `Repair-DeployRuleSetCompliance`, um die Regeln zu überprüfen und dem Host das richtige Image-Profil, Hostprofil oder den richtigen Ordnerspeicherort zuzuordnen.

Der Host wird nicht auf den Auto Deploy-Server umgeleitet

Während des Startens lädt ein Host, den Sie mit Auto Deploy bereitstellen möchten, iPXE. Der Host wird nicht auf den Auto Deploy-Server umgeleitet.

Problem

Während des Startens lädt ein Host, den Sie mit Auto Deploy bereitstellen möchten, iPXE. Der Host wird nicht auf den AutoDeploy-Server umgeleitet.

Ursache

Die Datei `tramp`, die in der TFTP-ZIP-Datei enthalten ist, enthält die falsche IP-Adresse für den Auto Deploy-Server.

Lösung

◆ Korrigieren Sie die IP-Adresse des Auto Deploy-Servers in der `tramp`-Datei. Weitere Informationen dazu finden Sie im *Installations- und Einrichtungshandbuch für vSphere*.

Der Auto Deploy-Host mit integriertem USB-Flash-Laufwerk sendet keine Coredumps an die lokale Festplatte

Wenn der Auto Deploy-Host über ein integriertes USB-Flash-Laufwerk verfügt und ein Fehler auftritt, der einen Coredump verursacht, geht der Coredump verloren. Richten Sie das System für die Verwendung von ESXi Dump Collector ein, um Coredumps auf einem vernetzten Host zu speichern.

Problem

Wenn der Auto Deploy-Host über ein integriertes USB-Flash-Laufwerk verfügt und ein Fehler auftritt, der einen Coredump verursacht, wird der Coredump nicht an die lokale Festplatte übermittelt.

Lösung

1. Installieren Sie ESXi Dump Collector auf einem System Ihrer Wahl.

   ESXi Dump Collector ist im vCenter Server-Installationsprogramm enthalten.

2. Verwenden Sie ESXCLI zum Konfigurieren des Hosts für die Verwendung von ESXi Dump Collector.

   ```
   esxcli conn_options system coredump network set IP-addr,port
   esxcli system coredump network set -e true
   ```

3. Verwenden Sie ESXCLI zum Deaktivieren lokaler Coredump-Partitionen.

   ```
   esxcli conn_options system coredump partition set -e false
   ```

Paket-Warnmeldung, wenn Sie dem Auto Deploy-Host ein Image-Profil zuweisen

Wenn Sie ein PowerCLI-cmdlet ausführen, dass ein Image-Profil zuweist, das nicht für Auto Deploy bereit ist, wird eine Warnmeldung angezeigt.

Problem

Wenn Sie Regeln definieren oder ändern, um einem oder mehreren Hosts ein Image-Profil zuzuweisen, tritt der folgende Fehler auf:

```
Warnung: Das Image-Profil <Name> enthält ein oder mehrere Softwarepakete, die nicht „stateless-
ready“ sind. Möglicherweise treten Probleme auf, wenn Sie dieses Profil mit Auto Deploy verwen-
den.
```

Ursache

Jedes VIB in einem Image-Profil hat ein `stateless-ready`-Flag, das angibt, dass das VIB zur Verwendung mit Auto Deploy gedacht ist. Sie erhalten den Fehler, wenn Sie versuchen, eine Auto Deploy-Regel zu schreiben, die ein Image-Profil verwendet, in dem bei einem oder mehreren VIBs das Flag auf FALSE gesetzt ist.

HINWEIS Sie können problemlos Hosts verwenden, die mit Auto Deploy bereitgestellt wurden und VIBs enthalten, die nicht „stateless-ready“ sind. Allerdings wird das Starten mit einem Image-Profil, das VIBs enthält, die nicht „stateless-ready“ sind, wie eine Neuinstallation behandelt. Jedes Mal, wenn Sie den Host starten, verlieren Sie Konfigurationsdaten, die anderenfalls auch nach Neustarts für mit Auto Deploy bereitgestellte Hosts verfügbar sein würden.

Lösung

1 Verwenden Sie Image Builder PowerCLI-cmdlets zum Anzeigen der VIBs im Image-Profil.

2 Entfernen Sie alle VIBs, die nicht „stateless-ready“ sind.

3 Führen Sie das Auto Deploy PowerCLI-cmdlet erneut aus.

Der Auto Deploy-Host wird nach fünf Minuten neu gestartet

Ein Auto Deploy-Host wird gestartet und zeigt iPXE-Informationen an, wird jedoch nach fünf Minuten neu gestartet.

Problem

Ein Host, der mit Auto Deploy bereitgestellt werden soll, wird von iPXE gestartet und zeigt iPXE-Informationen an der Konsole an. Nach fünf Minuten wird jedoch die folgende Meldung auf der Konsole angezeigt und der Host wird neu gestartet.

```
This host is attempting to network-boot using VMware
AutoDeploy. However, there is no ESXi image associated with this host.
Details: No rules containing an Image Profile match this
host. You can create a rule with the New-DeployRule PowerCLI cmdlet
and add it to the rule set with Add-DeployRule or Set-DeployRuleSet.
The rule should have a pattern that matches one or more of the attributes
listed below.
```

Der Host zeigt möglicherweise auch die folgenden Details an:

```
Details: This host has been added to VC, but no Image Profile
is associated with it. You can use Apply-ESXImageProfile in the
PowerCLI to associate an Image Profile with this host.
Alternatively, you can reevaluate the rules for this host with the
Test-DeployRuleSetCompliance and Repair-DeployRuleSetCompliance cmdlets.
```

Auf der Konsole werden dann die Attribute der Hostmaschine angezeigt, darunter Anbieter, Seriennummer, IP-Adresse usw.

Ursache

Derzeit ist diesem Host kein Image-Profil zugeordnet.

Lösung

Sie können dem Host temporär ein Image-Profil zuordnen, indem Sie das cmdlet `Apply-EsxImageProfile` ausführen.

Sie können dem Host ein permanentes Image-Profil wie folgt zuordnen.

1 Führen Sie das cmdlet `New-DeployRule` aus, um eine Regel zu erstellen, die ein Muster enthält, das dem Host ein Image-Profil zuordnet.

2 Führen Sie das cmdlet `Add-DeployRule` aus, um die Regel einem Regelsatz hinzuzufügen.

3 Führen Sie das cmdlet `Test-DeployRuleSetCompliance` aus und verwenden Sie die Ausgabe des cmdlets als Eingabe für das cmdlet `Repair-DeployRuleSetCompliance`.

Der Auto Deploy-Host führt keinen Netzwerkstart durch

Der Host, den Sie mit Auto Deploy bereitstellen, erscheint, führt jedoch keinen Netzwerkstart durch.

Problem

Wenn Sie versuchen, einen mit Auto Deploy bereitgestellten Host zu starten, startet der Host den Netzwerkstartvorgang nicht.

Ursache

Sie haben den Host für den Netzwerkstart nicht aktiviert.

Lösung

1 Starten Sie den Host neu und befolgen Sie die Anweisungen auf dem Bildschirm, um auf die BIOS-Konfiguration zuzugreifen.

   Wenn Sie einen EFI-Host einsetzen, müssen Sie das EFI-System in den BIOS-Kompatibilitätsmodus versetzen.

2 Aktivieren Sie den Netzwerkstart in der Konfiguration des Startgeräts der BIOS-Konfiguration.

Auto Deploy erhält keine von DHCP zugewiesene Adresse

Der Host, den Sie mit Auto Deploy bereitstellen, erhält keine DHCP-Adresse.

Problem

Wenn Sie versuchen, einen mit Auto Deploy bereitgestellten Host zu starten, führt der Host einen Netzwerkstart durch, ihm wird jedoch keine Adresse von DHCP zugewiesen. Der Auto Deploy-Server kann den Host mit dem Image-Profil nicht bereitstellen.

Ursache

Möglicherweise gibt es ein Problem mit dem DHCP-Dienst oder mit der Einrichtung der Firewall.

Lösung

1 Stellen Sie sicher, dass der DHCP-Serverdienst auf dem Windows-System ausgeführt wird, auf dem der DHCP-Server zum Bereitstellen von Hosts eingerichtet ist.

   a Klicken Sie auf **Start > Einstellungen > Systemsteuerung > Verwaltung**.

   b Doppelklicken Sie auf **Dienste**, um den Bereich „Dienstverwaltung“ zu öffnen.

   c Suchen Sie im Feld „Dienste“ nach dem DHCP-Serverdienst und starten Sie den Dienst neu, falls er nicht ausgeführt wird.

2 Wenn der DHCP-Server ausgeführt wird, überprüfen Sie den DHCP-Geltungsbereich und die DHCP-Reservierungen, die Sie für Ihre Zielhosts konfiguriert haben.

   Wenn der DHCP-Geltungsbereich und die DHCP-Reservierungen ordnungsgemäß konfiguriert sind, liegt das Problem wahrscheinlich bei der Firewall.

3 Um das Problem vorübergehend umzugehen, schalten Sie die Firewall aus, um festzustellen, ob dadurch das Problem behoben wurde.

   a Öffnen Sie die Eingabeaufforderung, indem Sie auf **Start > Programme > Zubehör > Eingabeaufforderung** klicken.

   b Geben Sie den folgenden Befehl ein, um die Firewall vorübergehend auszuschalten. Deaktivieren Sie die Firewall in Produktionsumgebungen nicht.

   ```
   netsh firewall set opmode disable
   ```

   c Versuchen Sie, den Host mit Auto Deploy bereitzustellen.

   d Geben Sie den folgenden Befehl ein, um die Firewall wieder einzuschalten.

   ```
   netsh firewall set opmode enable
   ```

4 Richten Sie Regeln ein, um den DHCP-Netzwerkdatenverkehr für die Zielhosts zu erlauben.

   Weitere Informationen dazu finden Sie in der Firewall-Dokumentation für DHCP und für das Windows-System, auf dem der DHCP-Server ausgeführt wird.

Der Auto Deploy-Host kann den TFTP-Server nicht kontaktieren

Der Host, den Sie mit Auto Deploy bereitstellen, kann den TFTP-Server nicht kontaktieren.

Problem

Wenn Sie versuchen, einen mit Auto Deploy bereitgestellten Host zu starten, führt der Host einen Netzwerkstart durch und erhält eine DHCP-Adresse vom DHCP-Server, aber der Host kann den TFTP-Server nicht kontaktieren.

Ursache

Der TFTP-Server wird möglicherweise nicht mehr ausgeführt, oder eine Firewall blockiert den TFTP-Port.

Lösung

- Wenn Sie den WinAgents TFTP-Server installiert haben, öffnen Sie den WinAgents TFTP-Verwaltungskonsole und stellen Sie sicher, dass der Dienst ausgeführt wird. Wenn der Dienst ausgeführt wird, überprüfen Sie die Windows-Firewallregeln für den eingehenden Datenverkehr, um sicherzugehen, dass der TFTP-Port nicht blockiert ist. Schalten Sie die Firewall vorübergehend aus, um festzustellen, ob das Problem bei der Firewall liegt.
- Sehen Sie im Falle aller anderen TFTP-Server in der Dokumentation zu Debuggen nach.

Auto Deploy Host kann kein ESXi -Image vom Auto Deploy-Server abrufen

Der Host, den Sie mit Auto Deploy bereitstellen, hält am iPXE-Startbildschirm an.

Problem

Wenn Sie versuchen, einen mit Auto Deploy bereitgestellten Host zu starten, wird der Startvorgang am iPXE-Startbildschirm angehalten und die Statusmeldung zeigt an, dass der Host versucht, das ESXi-Image vom Auto Deploy-Server abzurufen.

Ursache

Der Auto Deploy-Dienst wurde möglicherweise angehalten oder auf den Auto Deploy-Server kann nicht zugegriffen werden.

Lösung

1 Melden Sie sich bei dem System an, auf dem Sie den Auto Deploy-Server installiert haben.

2 Stellen Sie sicher, dass der Auto Deploy-Server ausgeführt wird.

   a Klicken Sie auf **Start > Einstellungen > Systemsteuerung > Verwaltung**.

   b Doppelklicken Sie auf **Dienste**, um den Bereich „Dienstverwaltung“ zu öffnen.

   c Suchen Sie im Feld „Dienste“ den Dienst „VMware vSphere Auto Deploy Waiter“ und starten Sie den Dienst erneut, falls er nicht bereits ausgeführt wird.

3 Starten Sie einen Webbrowser, geben Sie die folgende URL ein und überprüfen Sie, ob auf den Auto Deploy-Server zugegriffen werden kann.

   https://*IP-Adresse_des_Auto_Deploy_Servers*:*Port_des_Auto_Deploy_Servers*/vmw/rdb

   HINWEIS Verwenden Sie diese Adresse nur, um zu überprüfen, ob auf den Server zugegriffen werden kann.

4 Falls der Server nicht erreichbar ist, ist dies wahrscheinlich auf ein Firewall-Problem zurückzuführen.

   a Versuchen Sie, großzügige Regeln für den eingehenden TCP-Datenverkehr des Auto Deploy-Serverports einzurichten.

      Die Portnummer lautet 6501, es sei denn, Sie haben während der Installation eine andere Portnummer angegeben.

   b Als letztes Mittel deaktivieren Sie die Firewall vorübergehend und aktivieren Sie sie wieder, nachdem Sie festgestellt haben, ob sie den Datenverkehr blockiert hat. Deaktivieren Sie die Firewall in Produktionsumgebungen nicht.

      Führen Sie den Befehl `netsh firewall set opmode disable` zum Deaktivieren der Firewall aus. Führen Sie den Befehl `netsh firewall set opmode enable` zum Aktivieren der Firewall aus.

Wiederherstellen einer beschädigten Datenbank auf dem Auto Deploy-Server

In einigen Situationen tritt möglicherweise ein Problem bei der Auto Deploy-Datenbank auf. Die effizienteste Wiederherstellungsoption besteht darin, die vorhandene Datenbankdatei durch die letzte Sicherung zu ersetzen.

Problem

Wenn Sie Auto Deploy zum Bereitstellen der ESXi-Hosts in Ihrer Umgebung verwenden, tritt möglicherweise ein Problem bei der Auto Deploy-Datenbank auf.

WICHTIG Dieses Problem tritt nur selten auf. Führen Sie alle anderen Fehlerbehebungsstrategien für Auto Deploy aus, bevor Sie die aktuelle Datenbankdatei ersetzen. Regeln und Verknüpfungen, die Sie seit der ausgewählten Sicherung erstellt haben, gehen verloren.

Ursache

Dieses Problem tritt nur bei Hosts auf, die mit Auto Deploy bereitgestellt werden.

Lösung

1 Stoppen Sie den Auto Deploy-Server-Dienst.

2 Sie finden das Auto Deploy-Protokoll, indem Sie im vSphere Web Client zur Auto Deploy-Seite wechseln.

3 Durchsuchen Sie die Protokolle nach der folgenden Meldung:

```
DatabaseError: database disk image is malformed.
```

   Wenn Sie diese Meldung finden, ersetzen Sie die vorhandene Datenbank durch die letzte Sicherung.

4 Wechseln Sie zum Auto Deploy-Datenverzeichnis.

Betriebssystem	Dateispeicherort
vCenter Server Appliance	`/var/lib/rbd`
Microsoft Windows	Das Datenverzeichnis, das Sie während der Installation ausgewählt haben. Geben Sie zur Suche den folgenden Befehl in der Befehlszeile ein. `reg.exe QUERY "HKLM\SOFTWARE\WOW6432Node\VMware, Inc.\VMware vSphere Auto Deploy" /v DataPath`

Das Verzeichnis enthält eine Datei mit dem Namen `db` und Sicherungsdateien mit den Namen `db-`*jjj-mm-tt*.

5 Benennen Sie die aktuelle `db`-Datei um.

VMware Support wird Sie möglicherweise nach dieser Datei fragen, wenn Sie Assistenz anfordern.

6 Benennen Sie die letzte Sicherung in `db` um.

7 Starten Sie den Auto Deploy-Server-Dienst neu.

8 Falls die Meldung weiterhin im Protokoll erscheint, wiederholen Sie die Schritte, um die nächste letzte Sicherung zu verwenden, bis bei Verwendung von Auto Deploy keine Datenbankfehler mehr auftreten.

Machbarkeitsnachweis-Setup für Auto Deploy

Mithilfe einer Machbarkeitsnachweis-Einrichtung einer Auto Deploy-Umgebung können Administratoren das Produkt bewerten und seine Funktionen der Geschäftsführung vorstellen. Wenn Sie den Einrichtungs-workflow für den Machbarkeitsnachweis abgeschlossen haben, steht Ihnen eine funktionierende Auto Deploy-Umgebung mit einem Referenzhost und mindestens einem Zielhost zur Verfügung.

Das Machbarkeitsnachweis-Setup ist für eine Test- oder Entwicklungsumgebung vorgesehen, kann aber auch als Basis für eine Produktionsumgebung dienen. Die Aufgaben beginnen in einer Umgebung, in der keine Auto Deploy-Komponenten installiert sind. Die Aufgabenbeschreibungen gehen davon aus, dass Sie ein flaches Netzwerk ohne VLAN-Tagging zwischen den physischen Hosts und dem Rest Ihrer Umgebung verwenden.

Sie sollten über das folgende Hintergrundwissen und die entsprechenden Rechte verfügen, um die Aufgaben durchzuführen.

- Erfahrung mit vSphere (vCenter Server, ESX und ESXi).
- Grundkenntnisse der Microsoft PowerShell und vSphere PowerCLI.
- Administratorrechte auf die Windows- und vCenter Server-Zielsysteme.

Führen Sie die Aufgaben in der Reihenfolge durch, wie sie in diesem Dokument aufgeführt sind. Einige Schritte können in einer anderen Reihenfolge durchgeführt werden, aber die Reihenfolge, die hier verwendet wird, schränkt die Manipulation einiger Komponenten auf ein Mindestmaß ein.

Auto Deploy bietet keine End-to-End-Unterstützung für reine IPv6-Umgebungen. IPv6 wird von der PXE-Start-Infrastruktur nicht unterstützt. Nach der Bereitstellung können Sie die Hosts für die Verwendung von IPv6 manuell neu konfigurieren und dem vCenter Server über IPv6 hinzufügen. Beim Neustart eines status-freien Hosts geht die IPv6-Konfiguration allerdings verloren.

Checkliste für Machbarkeitsnachweis

Bevor Sie mit dem Machbarkeitsnachweis-Setup beginnen, vergewissern Sie sich, dass Ihre Umgebung die Hardware- und Softwareanforderungen erfüllt und Sie die erforderlichen Berechtigungen für die erforderlichen Komponenten besitzen.

Das Machbarkeitsnachweis-Setup ist auf vCenter Server 6.0 und höher ausgelegt. Für frühere Versionen von vCenter Server gehen Sie zum betreffenden VMware Documentation Center.

Für das Machbarkeitsnachweis-Setup muss Ihr System bestimmte Software- und Hardwareanforderungen erfüllen.

Tabelle 4-13. Checkliste vor der Installation

Erforderliche Software und Hardware	Details
Betriebssystem	Unterstütztes Windows-Betriebssystem (Windows Server 2008 R2 oder höher) mit vorinstallierter Microsoft PowerShell. Eine vollständige Liste der unterstützten Betriebssysteme finden Sie unter Unterstützte Hostbetriebssysteme für die VMware vCenter Server-Installation.
vCenter Server	Version 6.0 oder höher zur Installation auf einem Windows-System. Sie können vSphere PowerCLI auch auf einem anderen Windows-System installieren. Der Auto Deploy-Server ist Teil von vCenter Server. vSphere PowerCLI wird auf demselben Windows-System installiert. Viele Setupaufgaben können ausgeführt werden, indem Sie sich bei diesem System entweder direkt in der Konsole oder unter Verwendung von Remote Desktop (RDP) anmelden.
Speicher	Mindestens 4 GB freier Speicherplatz auf dem Windows-System, auf dem vCenter Server ausgeführt wird. Ein zweites Volume oder eine zweite Festplatte wird empfohlen. Speicher für ESXi-Datenspeicher (NFS, iSCSI oder Fibre Channel) mit Servern und Speicherarrays, die so konfiguriert sind, dass die Server die LUNs erkennen können ■ Eine Liste der Ziel-IP-Adressen für NFS oder iSCSi ■ Eine Liste mit Informationen über Ziel-Volumes für NFS oder iSCSi
Hostinformationen (für zwei oder mehrere Hosts)	Eine Liste der Ziel-IP-Adressen für NFS oder iSCSi Eine Liste mit Informationen über Ziel-Volumes für NFS oder iSCSi ■ Standardroute, Netzmaske und IP-Adressen für primäre und sekundäre DNS-Server ■ IP-Adresse und Netzmaske für das primäre VMkernel-Verwaltungsnetzwerk ■ IP-Adresse und Netzmaske für andere VMkernel-Netzwerke, wie Speicher, vSphere FT oder VMware vMotion Auto Deploy überschreibt vorhandene Partitionen nicht standardmäßig.
vSphere PowerCLI	Von der Downloads-Seite der VMware-Website heruntergeladene Binärdateien des vSphere PowerCLI-Installationsprogramms
ESXi-Softwaredepot	Der Ort des ESXi-Softwaredepots auf der Downloads-Seite der VMware-Website. Sie verweisen über eine URL auf das dort gespeicherte Image-Profil oder laden eine ZIP-Datei herunter und arbeiten mit einem lokalen Depot. Laden Sie das ESXi-Image nicht herunter.
TFTP-Server	TFTP-Installationssoftware wie zum Beispiel WinAgents TFTP-Server. Der in Windows Server 2008 enthaltene TFTP-Server ist eng mit der Windows-Netzwerkbereitstellung verknüpft und daher nicht geeignet.
DHCP-Server	Der in Windows Server 2008 enthaltene DHCP-Server ist für dieses Machbarkeitsnachweis-Setup geeignet.

Sie benötigen ebenfalls Informationen zu und Administratorrechte für die Hauptserver der Umgebung. Dazu zählen der ActiveDirectory-Server, der DNS-Server, der DHCP-Server, der NTP-Server usw.

Die Broadcast-Domäne des Subnetzes, in dem Sie das Setup bereitstellen, muss vollständig von Ihnen gesteuert werden können. Stellen Sie sicher, dass sich keine anderen DHCP-, DNS- oder TFTP-Server in diesem Subnetz befinden.

Installieren des TFTP-Servers

Auto Deploy stützt sich auf einen TFTP-Server zum Senden des Start-Images an die Hosts, die es bereitstellt. Sie müssen einen TFTP-Server in Ihrer Umgebung installieren.

Diese Aufgabe installiert nur den TFTP-Server. Später laden Sie eine Konfigurationsdatei auf den Server herunter. Siehe „Konfigurieren der Auto Deploy- und TFTP-Umgebung im vSphere Web Client“, auf Seite 141.

Voraussetzungen

Stellen Sie sicher, dass Ihr System die Anforderungen in der Vorinstallations-Checkliste erfüllt. Siehe „Checkliste für Machbarkeitsnachweis“, auf Seite 135.

Vorgehensweise

1 Melden Sie sich entweder direkt oder über RDP mit Administratorrechten bei der Konsole des Windows-Systems an, auf dem vCenter Server installiert ist.

2 Laden Sie die TFTP-Server-Software herunter und installieren Sie sie.

   Dieses Beispiel-Setup verwendet den TFTP-Server von WinAgents. Der im Lieferumfang von Windows 2008 enthaltene TFTP-Server ist eher für das Bereitstellen in Windows-Netzwerken konzipiert und daher für Auto Deploy nicht geeignet.

3 Konfigurieren Sie das TFTP-Stammverzeichnis als D:*Laufwerk* oder ähnlich (Beispiel: `D:\TFTP_Root\`).

Weiter

Installieren und Einrichten von vSphere PowerCLI Sie verwenden PowerCLI-cmdlets, um Regeln zu erstellen, die den Hosts Image-Profilen bereit und Hostprofile zuweisen. Siehe „Installieren und Einrichten von vSphere PowerCLI“, auf Seite 137.

Installieren und Einrichten von vSphere PowerCLI

Sie verwalten Auto Deploy anhand von Regeln, die Sie mithilfe von vSphere PowerCLI-cmdlets erstellen.

Dieses Machbarkeitsnachweis-Setup installiert vSphere PowerCLI auf demselben System wie das vCenter Server-System. Sie können vSphere PowerCLI auch auf einem anderen Windows-System installieren.

Voraussetzungen

- Stellen Sie sicher, dass Microsoft .NET 4.5 SP2 installiert ist, oder installieren Sie es von der Microsoft-Website aus.
- Stellen Sie sicher, dass Windows PowerShell 3.0 installiert ist, oder installieren Sie es von der Microsoft-Website aus.

Vorgehensweise

1 Melden Sie sich entweder direkt oder über RDP mit Administratorrechten bei der Konsole des Windows-Systems an, auf dem vCenter Server installiert ist.

2 Laden Sie vSphere PowerCLI von der Downloadseite der VMware-Website herunter und installieren Sie die vSphere PowerCLI-Software.

3 Stellen Sie sicher, dass vSphere PowerCLI ausgeführt wird.

   a Doppelklicken Sie auf das vSphere PowerCLI-Symbol auf dem Desktop, um ein vSphere PowerCLI-Fenster zu öffnen.

   b (Optional) Wenn ein SSL-Fehler eingeblendet wird, prüfen Sie den Fingerabdruck und ignorieren Sie den Fehler, führen Sie dann den Befehl `Get-DeployCommand` aus und drücken Sie die Eingabetaste.

   vSphere PowerCLI zeigt eine Liste von cmdlets und deren Definitionen im vSphere PowerCLI-Fenster an.

Weiter

- Falls keine Liste von cmdlets erscheint, wenn Sie `Get-DeployCommand` ausführen, überprüfen Sie Ihre vSphere PowerCLI-Version und bei Bedarf deinstallieren Sie sie und installieren Sie sie neu.
- Einige Hintergrundinformationen zu vSphere PowerCLI finden Sie unter „Verwendung der Auto Deploy-cmdlets“, auf Seite 90. Details finden Sie im *vSphere PowerCLI-Benutzerhandbuch*.
- Bereiten Sie die Hosts, die Sie bereitstellen möchten, mit Auto Deploy vor. Siehe „Vorbereiten von Zielhosts für Auto Deploy“, auf Seite 138.

Vorbereiten von Zielhosts für Auto Deploy

Sie müssen alle Zielhosts für Auto Deploy vorbereiten.

Voraussetzungen

Hosts, die mit Auto Deploy bereitgestellt werden sollen, müssen die Anforderungen für ESXi erfüllen.

Weitere Informationen hierzu finden Sie unter „Hardwareanforderungen für ESXi“, auf Seite 21.

HINWEIS Sie können keine EFI-Hosts mit Auto Deploy bereitstellen, es sei denn, Sie versetzen die EFI-Systeme in den BIOS-Kompatibilitätsmodus.

Vorgehensweise

1 Ändern Sie die BIOS-Einstellungen für jeden einzelnen physischen Host, um das Starten des Hosts über das primäre Netzwerkgerät zu erzwingen.

2 Bestätigen Sie die MAC-Adresse des primären Netzwerkgeräts erneut.

Weiter

Bereiten Sie den DHCP-Server vor. Weitere Informationen hierzu finden Sie unter „Vorbereiten des DHCP-Servers“, auf Seite 138.

Vorbereiten des DHCP-Servers

Der DHCP-Server in Ihrer Beispielumgebung muss so eingerichtet werden, dass er jedem Zielhost eine iPXE-Binärdatei zur Verfügung stellt.

Die Beispielumgebung verwendet Active Directory mit DNS und DHCP.

Dieses Beispiel stellt die Verwendung von DHCP-Reservierungen dar. Das Einrichten von festen IP-Adressen für jeden Host ist zeitintensiv und wird nicht empfohlen.

Voraussetzungen

- Stellen Sie sicher, dass Ihr System die Anforderungen in der Vorinstallations-Checkliste erfüllt. Siehe „Checkliste für Machbarkeitsnachweis“, auf Seite 135.

- Führen Sie alle vorangegangenen Machbarkeitsnachweis-Setupaufgaben durch. Die vollständige Liste finden Sie unter „Machbarkeitsnachweis-Setup für Auto Deploy“, auf Seite 135.

Vorgehensweise

1 Melden Sie sich als Administrator an Ihrem DHCP-Server an.

2 Erstellen Sie einen DHCP-Bereich für Ihren IP-Adressbereich.

   a Klicken Sie auf **Start > Einstellungen > Systemsteuerung > Verwaltung** und dann auf **DHCP**.

   b Gehen Sie zu **DHCP > *Hostname* > IPv4**.

   c Klicken Sie mit der rechten Maustaste auf **IPv4** und wählen Sie **Neuer Bereich**.

   d Klicken Sie im Begrüßungsbildschirm auf **Weiter** und geben Sie einen Namen und eine Beschreibung für den Bereich an.

   e Geben Sie den IP-Adressbereich an und klicken Sie auf **Weiter**.

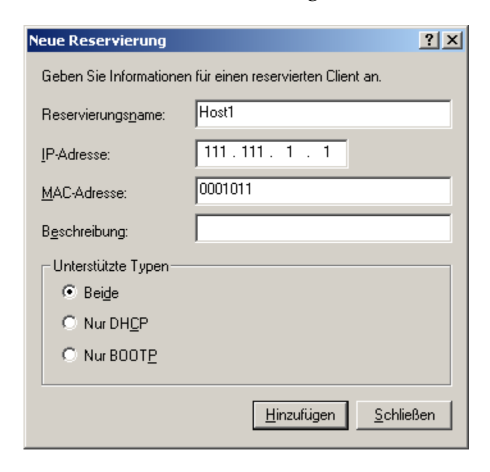
   f Klicken Sie so lange auf **Weiter**, bis der Bildschirm „DHCP-Optionen konfigurieren“ angezeigt wird, und wählen Sie **Nein, ich möchte diese Option später konfigurieren** aus.

3 Wenn Sie DHCP-Reservierungen zukünftig verwenden möchten, erstellen Sie eine DHCP-Reservierung für jeden Ziel-ESXi-Host.

   a Gehen Sie im DHCP-Fenster zu **DHCP > *Hostname* > IPv4 > Auto Deploy-Bereich > Reservierungen**.

   b Klicken Sie mit der rechten Maustaste auf **Reservierungen** und wählen Sie **Neue Reservierung** aus.

   c Geben Sie im Fenster „Neue Reservierung“ einen Namen, eine IP-Adresse und die MAC-Adresse für einen der Hosts ein. Fügen Sie keinen Doppelpunkt (:) in die MAC-Adresse ein.



   d Wiederholen Sie den Vorgang für alle anderen Hosts.

4 Richten Sie den DHCP-Server ein, um die Hosts zum TFTP-Server zu verweisen.

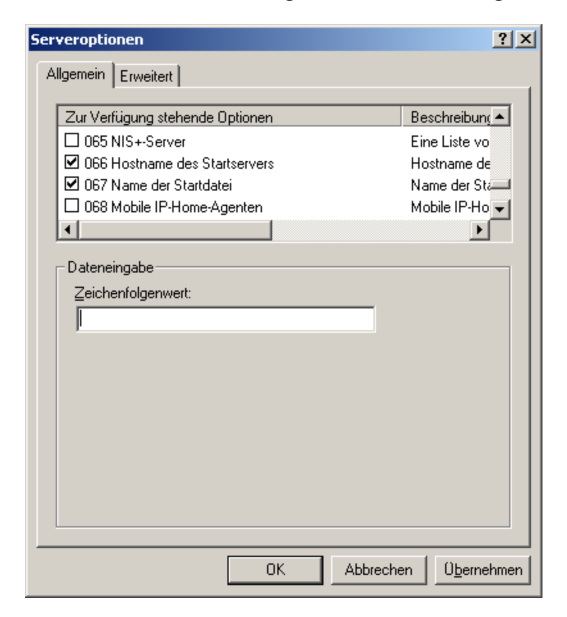
   Der jeweilige Vorgang richtet sich nach dem verwendeten DHCP-Server. In diesem Beispiel wird der in Windows 2008 enthaltene DHCP-Server verwendet.

   a Gehen Sie im DHCP-Fenster zu **DHCP > *Hostname* > IPv4 > Auto Deploy-Bereich > Bereichsoptionen**.

   b Klicken Sie mit der rechten Maustaste auf **Bereichsoptionen** und wählen Sie **Optionen konfigurieren** aus.

   c Klicken Sie im Fenster „Bereichsoptionen“ auf die Registerkarte**Allgemein**.

d Klicken Sie auf **066 Startserver-Hostname** und geben Sie die Adresse des TFTP-Servers ein, den Sie im Wertfeld „Zeichenfolge“ unter den verfügbaren Optionen installiert haben.



e Klicken Sie auf **067 Startdateiname** und geben Sie **`undionly.kpxe.vmw-hardwired`** ein.

Die iPXE-Binärdatei `undionly.kpxe.vmw-hardwired` wird zum Starten der ESXi-Hosts verwendet.

f Klicken Sie auf **Übernehmen** und anschließend auf **OK**, um das Fenster zu schließen.

5 Klicken Sie im DHCP-Fenster mit der rechten Maustaste auf **DHCP > *Hostname* > IPv4 > Bereich > aktivieren** und klicken Sie dann auf**Aktivieren**.

6 Melden Sie sich nicht vom DHCP-Server ab, wenn Sie Active Directory für DHCP und DNS verwenden.

Weiter

Bereiten Sie den DNS-Server vor. Siehe „Vorbereiten des DNS-Servers“, auf Seite 140.

Vorbereiten des DNS-Servers

Die Vorbereitung des DNS-Servers schließt das Hinzufügen von DHCP-Informationen zum DSN-Server sowie die Überprüfung der Funktionalität der DNS-Einträge ein. Dieser Vorgang ist optional.

Die Beispielumgebung verwendet Active Directory mit DNS und DHCP.

Voraussetzungen

Führen Sie alle vorangegangenen Machbarkeitsnachweis-Setupaufgaben durch. Die vollständige Liste finden Sie unter „Machbarkeitsnachweis-Setup für Auto Deploy“, auf Seite 135.

Vorgehensweise

1 Melden Sie sich am DNS-Server an.

2 Fügen Sie die IP-Adressen für die DHCP-Reservierung und die zugehörigen Hostnamen als statische DNS-Einträge hinzu.

   Fügen Sie die Einträge zu den Zonen Forward (ARecord) und Reverse (PTR Record) hinzu.

3 Melden Sie sich entweder direkt oder über RDP mit Administratorrechten bei der Konsole des Windows-Systems an, auf dem vCenter Server installiert ist.

4 Öffnen Sie eine Befehlszeile und führen Sie einen nslookup-Befehl für die ESXi-Hostnamen durch, um zu überprüfen, ob die DNS-Einträge funktionieren.

   Führen Sie ein Forward- (Short und FQDN) und ein Reverse-Lookup durch.

5 Melden Sie sich von Ihrem DNS-Server ab.

Konfigurieren der Auto Deploy- und TFTP-Umgebung im vSphere Web Client

Sie müssen eine TFTP-Startdatei (ZIP-Format) von Ihrem Auto Deploy-Server herunterladen. Der angepasste FTP-Server stellt die Start-Images bereit, die Auto Deploy zur Verfügung stellt. Sie können die folgende Aufgabe im vSphere Web Client ausführen.

Voraussetzungen

- Stellen Sie sicher, dass Ihr System die Anforderungen in der Vorinstallations-Checkliste erfüllt. Siehe „Checkliste für Machbarkeitsnachweis“, auf Seite 135.
- Führen Sie alle vorangegangenen Machbarkeitsnachweis-Setupaufgaben durch. Die vollständige Liste finden Sie unter „Machbarkeitsnachweis-Setup für Auto Deploy“, auf Seite 135.

Vorgehensweise

1 Greifen Sie in Ihrem Webbrowser auf die URL des vSphere Web Client zu, der eine Verbindung zu dem vCenter Server-System hat, das den Auto Deploy-Server verwaltet.

2 Wenn die Zertifikatswarnung angezeigt wird, fahren Sie mit dem vCenter Server-System fort.

3 Starten Sie den Auto Deploy-Dienst.

   a Klicken Sie auf der Startseite von vSphere Web Client auf **Verwaltung**.

   b Klicken Sie unter **Systemkonfiguration** auf **Dienste**.

   c Wählen Sie **Auto Deploy** aus, klicken Sie auf das Menü **Aktionen** und wählen Sie **Starten** aus.

      Unter Windows kann der Auto Deploy-Dienst deaktiviert werden. Sie können den Dienst durch Ändern des Starttyps des Auto Deploy-Diensts aktivieren.

4 Gehen Sie in der Bestandsliste zum vCenter Server-System.

5 Wählen Sie auf der Registerkarte „Verwalten “ die Option **Einstellungen** aus und klicken Sie auf **Auto Deploy**.

6 Klicken Sie auf den Link **TFTP Boot Zip herunterladen**, um die TFTP-Konfigurationsdatei herunterzuladen.

7 Speichern Sie die Datei `Deploy-tftp.zip` in dem `TFTP_Root`-Verzeichnis, das Sie beim Installieren des TFTP-Servers erstellt haben, und entpacken Sie die Datei.

8 Minimieren Sie den Webbrowser, den Sie mit dem vSphere Web Client verwenden.

Weiter

Bereiten Sie das Depot vor, aus dem Auto Deploy die ESXi abruft, wenn es die Hosts bereitstellt. Weitere Informationen hierzu finden Sie unter „Vorbereiten des ESXi-Software-Depots“, auf Seite 142.

Vorbereiten des ESXi-Software-Depots

Auto Deploy stellt Hosts die in Image-Profilen beschriebenen Images bereit. Image-Profile werden in Software-Depots gespeichert. Sie müssen sicherstellen, dass das richtige Image-Profil vor der Bereitstellung der Hosts verfügbar ist.

Das ESXi-Software-Depot beinhaltet die Image-Profile und die Softwarepakete (VIBs), die zur Ausführung von ESXi verwendet werden. Ein Image-Profil ist eine Liste von VIBs. Dieses Beispielsetup verwendet ein von VMware bereitgestelltes Depot und Image-Profil, es erstellt jedoch keine benutzerdefinierten Image-Profile.

Dieses Beispielsetup lädt die ZIP-Datei mit dem Image-Profil herunter. Stattdessen können Sie den Auto Deploy-Server zur HTTP-URL eines Image-Profils leiten.

Wenn Sie benutzerdefinierte VIBs als benutzerdefinierte Treiber in Ihrem Image-Profil benötigen, können Sie ein benutzerdefiniertes Image-Profil mit der Image Builder-PowerCLI erstellen.

Die Schritte in dieser Aufgabe dienen zur Ausführung der PowerCLI-cmdlets. Wenn Sie weitere Informationen zu jedem cmdlet benötigen, geben Sie an der PowerCLI-Eingabeaufforderung `Help` *cmdlet* ein oder durchsuchen Sie das vSphere Documentation Center.

Voraussetzungen

- Stellen Sie sicher, dass Ihr System die Anforderungen in der Vorinstallations-Checkliste erfüllt. Siehe „Checkliste für Machbarkeitsnachweis“, auf Seite 135.
- Führen Sie alle vorangegangenen Machbarkeitsnachweis-Setupaufgaben durch. Die vollständige Liste finden Sie unter „Machbarkeitsnachweis-Setup für Auto Deploy“, auf Seite 135.

Vorgehensweise

1. Melden Sie sich entweder direkt oder über RDP mit Administratorrechten bei der Konsole des Windows-Systems an, auf dem vCenter Server installiert ist.
2. Laden Sie die komprimierte ESXi-Depot-Datei (.zip) von der VMware-Website in ein Verzeichnis herunter, auf das das PowerCLI-Windows-System zugreifen kann.

   Die Datei weist einen Namen mit folgendem Muster auf: `VMware-Esxi-N.N.N-xxxxx-depot.zip`.
3. Speichern Sie die ZIP-Datei auf Ihrem lokalen D:\-Laufwerk oder einem beliebigen Datenträger mit ausreichend Speicherkapazität und notieren Sie sich das Verzeichnis.
4. Starten Sie eine PowerCLI-Sitzung und führen Sie die folgenden cmdlets an der Eingabeaufforderung aus.

   ```
   Connect-VIServer -Server your_vc_hostname -User username -Password password <Enter>
   Add-EsxSoftwareDepot path:\VMware-Esxi-version-xxxxx-depot.zip <Enter>
   ```

   Geben Sie den vollständigen Pfad und den Dateinamen der ZIP-Datei an, die Sie zuvor heruntergeladen haben.
5. Stellen Sie sicher, dass Sie die ZIP-Datei erfolgreich zum Depot hinzugefügt haben, indem Sie die Inhalte des Depots mit dem cmdlet`Get-EsxImageProfile` überprüfen.

   ```
   Get-EsxImageProfile <Enter>
   ```

   Das cmdlet gibt Informationen zu allen Image-Profilen im Depot zurück.

Weiter

Richten Sie Auto Deploy ein, um den ersten Host bereitzustellen. Stellen Sie diesem Host anschließend das Image-Profil im Depot bereit. Siehe „Einrichten des ersten Hosts und Bereitstellen mit Auto Deploy“, auf Seite 143.

Einrichten des ersten Hosts und Bereitstellen mit Auto Deploy

Wenn Sie den ersten Host einrichten, müssen Sie wissen, wie Auto Deploy-Regeln mit vSphere PowerCLI geschrieben werden. Nach dem Schreiben der Regeln und Hinzufügen zum Regelsatz, können Sie den Host zur Bereitstellung einschalten.

Sie können die PowerCLI-Befehlszeilenschnittstelle verwenden, um festzulegen, wie die Zielhosts von Auto Deploy bereitgestellt werden. Sie legen Regeln fest und fügen jede Regel zum aktiven Regelsatz hinzu. Der Auto Deploy-Server prüft den Regelsatz, um festzulegen, welches Image-Profil und Hostprofil an jeden ESXi-Host gesendet und in welchem Verzeichnis der Host auf dem vCenter Server gespeichert werden soll.

Mit einer Regel können Sie die folgenden Parameter festlegen.

Parameter	Beschreibung
Name	Name der mit dem`–Name`-Parameter festgelegten Regel.
Element	Ein oder mehrere mit dem `–Item`-Parameter festgelegten Elemente. Ein Element kann ein zu verwendendes Image-Profil oder ein vCenter Server-Bestandslistenspeicherort (Datencenter, Ordner, Cluster) für den Zielhost sein. Sie können mehrere Elemente durch Komma getrennt angeben.
Muster	Das Muster gibt den Host oder die Hostgruppe an, für die die Regel angewendet wird. Wählen Sie aus folgenden Optionen aus. **Anbieter** – Anbietername der Maschine. **Modell** – Modellbezeichnung der Maschine. **Seriell** – Seriennummer der Maschine. **Hostname** – Hostname der Maschine. **domain** – Domänenname. **ipv4** – IPv4-Adresse der Maschine. **Mac** – MAC-Adresse der Startnetzwerkkarte. **Asset** – Asset-Tag der Maschine. **oemstring** – OEM-spezifische Zeichenfolgen im SMBIOS. Legen Sie `–AllHosts` fest, um das Element oder die Elemente auf alle Hosts anzuwenden.

In diesem Beispielsetup wird `–AllHosts` und anschließend ein IP-Adressbereich verwendet, um die bereitzustellenden Hosts anzugeben.

Erstellen Sie Regeln für den ersten Host

Legen Sie zunächst mit Hilfe von PowerCLI das Image-Profil fest, das auf dem Host bereitgestellt werden soll, indem Sie eine entsprechende Regel erstellen und diese dem aktiven Regelsatz hinzufügen.

Bei dieser Aufgabe wird davon ausgegangen, dass Sie über grundlegende Kenntnisse der Microsoft PowerShell und vSphere PowerCLI verfügen.

Voraussetzungen

- Stellen Sie sicher, dass Ihr System die Anforderungen in der Vorinstallations-Checkliste erfüllt. Siehe „Checkliste für Machbarkeitsnachweis“, auf Seite 135.
- Führen Sie alle vorangegangenen Machbarkeitsnachweis-Setupaufgaben durch. Die vollständige Liste finden Sie unter „Machbarkeitsnachweis-Setup für Auto Deploy“, auf Seite 135.
- Stellen Sie sicher, dass Sie auf die ESXi-Software des Systems, auf dem Sie die PowerCLI-cmdlets ausführen, zugreifen können.

Vorgehensweise

1. Melden Sie sich entweder direkt oder über RDP mit Administratorrechten bei der Konsole des Windows-Systems an, auf dem vCenter Server installiert ist.

   Bei dieser Aufgabe wird davon ausgegangen, dass PowerCLI auf dem System installiert ist, auf dem das vCenter Server-System ausgeführt wird.

2. Öffnen Sie das PowerCLI-Fenster und rufen Sie das ESXi-Image-Profil auf.

   ```
   Get-EsxImageProfile
   ```

3. Erstellen Sie durch das Aufrufen des folgenden Cmdlets eine neue Regel, indem Sie „ESXi-5.1.0-*XXXXX*-standard“ durch das gewünschte Image-profil ersetzen.

   ```
   New-DeployRule -Name "InitialBootRule" -Item "Esxi-5.1.0-XXXXX-standard" -AllHosts
   ```

4. Fügen Sie die neue Regel dem aktiven Regelsatz hinzu, um dem Auto Deploy-Server die Regel verfügbar zu machen.

   ```
   Add-DeployRule -DeployRule "InitialBootRule"
   ```

Weiter

Starten Sie den Host und prüfen Sie die Bereitstellung des Hosts durch Auto Deploy und die Verfügbarkeit des Hosts in der vCenter Server-Bestandsliste. Siehe „Bereitstellen des ersten Hosts“, auf Seite 144.

Bereitstellen des ersten Hosts

Sie können den ersten Host bereitstellen und seinen Speicherort auf dem vCenter Server überprüfen, um die Überprüfung der Image-Bereitstellung Ihres Setups abzuschließen.

Voraussetzungen

- Stellen Sie sicher, dass Ihr System die Anforderungen in der Vorinstallations-Checkliste erfüllt. Siehe „Checkliste für Machbarkeitsnachweis“, auf Seite 135.
- Führen Sie alle vorangegangenen Machbarkeitsnachweis-Setupaufgaben durch. Die vollständige Liste finden Sie unter „Machbarkeitsnachweis-Setup für Auto Deploy“, auf Seite 135.

Vorgehensweise

1. Öffnen Sie eine Konsolensitzung zum physischen Host, den Sie als ersten ESXi-Zielhost verwenden möchten, starten Sie den Host und suchen Sie nach Nachrichten, die auf einen erfolgreichen iPXE-Start hindeuten.

   Während des Startvorgangs weist DHCP dem Host eine IP-Adresse zu. Die IP-Adresse stimmt mit einem Namen überein, den Sie zu einem früheren Zeitpunkt im DNS-Server angegeben haben. Der Host stellt einen Kontakt zum Auto Deploy-Server her und lädt die ESXi-Binärdateien über die HTTP-URL herunter, die in der iPXE-tramp-Datei angegeben sind, die Sie zu einem früheren Zeitpunkt in das TFTP_Root-Verzeichnis heruntergeladen haben. Jede Instanz von Auto Deploy erstellt eine benutzerdefinierte Gruppe von Dateien für den TFTP-Server.

2. Stellen Sie mit einem vSphere Web Client eine Verbindung mit dem vCenter Server-System her.

   Das vCenter Server-System in diesem Machbarkeitsnachweis-Setup ist „localhost“.

3. Klicken Sie auf **Hosts und Cluster**.

4. Stellen Sie sicher, dass sich der neu bereitgestellte Host jetzt in der vCenter Server-Bestandsliste auf der Datencenterebene befindet.

   Beim Abschließen des Startvorgangs fügt Auto Deploy standardmäßig Hosts auf der Datencenterebene hinzu.

Weiter

Im Problemfall finden Sie weiterführende Informationen unter „Fehlerbehebung bei Auto Deploy“, auf Seite 129.

Konfigurieren Sie den ersten Host als Referenzhost und speichern Sie das Hostprofil so, dass es von anderen Hosts verwendet werden kann. Siehe „Konfigurieren des Machbarkeitsnachweis-Referenzhosts“, auf Seite 145.

Konfigurieren des Machbarkeitsnachweis-Referenzhosts

Sie können den ersten ESXi-Host, den Sie für Ihre Umgebung starten, anpassen und ein Hostprofil erstellen. Sie können Auto Deploy für das Bereitstellen von anderen Zielhosts mit diesem Hostprofil einrichten. Der ESXi-Host, von dem Sie das Hostprofil erstellen, wird als Referenzhost oder Vorlagen-Host bezeichnet.

Wie Sie den Referenzhost konfigurieren, hängt von dem ab, was Sie tun möchten.

Gemeinsam genutzte Einstellungen
Geben Sie die Einstellungen an, die von allen Hosts gemeinsam genutzt werden, und speichern Sie ein Hostprofil für den Host.

Hostspezifische Einstellungen
Sie können Hosts anpassen, indem Sie das Hostprofil so einrichten, dass für eine begrenzte Anzahl von Optionen, wie z. B. eine statische IP-Adresse, der Benutzer aufgefordert wird, eine Eingabe vorzunehmen. Hostanpassungen werden gespeichert, wenn Sie das Hostprofil speichern. Siehe „Hostanpassung im vSphere Web Client“, auf Seite 118.

Auto Deploy wendet alle gemeinsam genutzten Einstellungen aus dem Hostprofil auf alle Zielhosts an. Wenn Sie das Hostprofil so einrichten, dass der Benutzer aufgefordert wird, Eingaben vorzunehmen, werden alle mit diesem Hostprofil bereitgestellten Hosts im Wartungsmodus gestartet. Sie müssen das Hostprofil neu anwenden oder die Hostanpassungen zurücksetzen, damit der Benutzer aufgefordert wird, die hostspezifischen Informationen einzugeben.

HINWEIS Administratoren können weder direkt auf Hostanpassungen zugreifen noch diese manipulieren. Verwenden Sie die Hostprofil-Benutzeroberfläche des vSphere Web Client, um mit Hostanpassungen zu arbeiten.

Voraussetzungen

- Stellen Sie sicher, dass Ihr System die Anforderungen in der Vorinstallations-Checkliste erfüllt. Siehe „Checkliste für Machbarkeitsnachweis“, auf Seite 135.
- Führen Sie alle vorangegangenen Machbarkeitsnachweis-Setupaufgaben durch. Die vollständige Liste finden Sie unter „Machbarkeitsnachweis-Setup für Auto Deploy“, auf Seite 135.

Vorgehensweise

1. Verwenden Sie den vSphere Web Client zum Herstellen einer Verbindung mit dem vCenter Server-System.

   Das vCenter Server-System in diesem Machbarkeitsnachweis-Setup ist „localhost“.

2. Klicken Sie auf „Hosts und Cluster“ und wählen Sie den Host aus, den Auto Deploy zum ersten Datencenter hinzugefügt hat.

3 Konfigurieren Sie den Host.

Beim Rest des Machbarkeitsnachweis-Setups wird davon ausgegangen, dass Sie mindestens eine Einstellung konfigurieren, die sich für unterschiedliche Hosts unterscheidet.

Konfiguration	Beschreibung
Netzwerk	Konfigurieren Sie die folgenden Netzwerkkomponenten. ■ Virtueller Basis-Switch und die Verwaltungs-Portgruppe für VMkernel. ■ Speichernetzwerk-Portgruppe für VMkernel. ■ Portgruppe für das Netzwerk virtueller Maschinen. ■ Eventuell zusätzliche virtuelle Switches und Portgruppen. ■ Distributed Switches, falls erforderlich (übertragen Sie die Portgruppen auf Distributed Switches, falls Sie sie verwenden).
Speicher	Konfigurieren Sie gemeinsam genutzten Speicher.
Uhrzeiteinstellungen	Konfigurieren Sie die Datums- und Uhrzeiteinstellungen.
Sicherheit	Konfigurieren Sie das Sicherheitsprofil.
Authentifizierung	Konfigurieren Sie die Authentifizierung.
DNS und Routing	Falls erforderlich, konfigurieren Sie DNS und die Routeneinstellungen.
Andere	Konfigurieren Sie die erweiterten Einstellungen oder andere Einstellungen, die für die Zielumgebung erforderlich sind.

Weiter

Erstellen Sie das Hostprofil anhand des Referenzhosts für die Verwendung mit allen anderen Zielhosts. Weitere Informationen finden Sie in der Dokumentation *Hostprofile*.

Erstellen und Anwenden eines Hostprofils mit dem vSphere Web Client

Eine Konfiguration, die von einer Gruppe von Hosts gemeinsam genutzt wird, wird in einem Hostprofil gespeichert. Sie können das Hostprofil anhand Ihres Referenzhosts erstellen. Ein Konfigurationswert, der sich bei verschiedenen Hosts unterscheidet, wie z. B. eine statische IP-Adresse, kann über den Hostanpassungsmechanismus verwaltet werden.

Auto Deploy stellt jeden Host mit demselben Hostprofil bereit. In bestimmten Fällen verwendet Auto Deploy auch Hostanpassungen, die es Ihnen ermöglicht, jeweils unterschiedliche Informationen für unterschiedliche Hosts anzugeben. Wenn Sie beispielsweise einen VMkernel-Port für vMotion oder für Speicher einrichten, können Sie unter Verwendung des Hostanpassungsmechanismus eine statische IP-Adresse für den Port angeben.

In diesem Beispiel extrahieren Sie ein Hostprofil aus einem Referenzhost, hängen Sie das Hostprofil an einen anderen Host an und überprüfen Sie die Hostprofilübereinstimmung. In den meisten Fällen führen Sie diese Aufgaben nicht manuell aus, sondern Sie schreiben eine Auto Deploy-Regel, die ein Hostprofil an Hosts anhängt, die mit Auto Deploy bereitgestellt werden. Weitere Informationen hierzu finden Sie unter „Erstellen einer Regel und Zuweisen eines Hostprofils zu Hosts“, auf Seite 94.

Voraussetzungen

- Stellen Sie sicher, dass Ihr System die Anforderungen in der Vorinstallations-Checkliste erfüllt. Siehe „Checkliste für Machbarkeitsnachweis“, auf Seite 135.
- Führen Sie alle vorangegangenen Machbarkeitsnachweis-Setupaufgaben durch. Die vollständige Liste finden Sie unter „Machbarkeitsnachweis-Setup für Auto Deploy“, auf Seite 135.

Vorgehensweise

1 Melden Sie sich an einen vSphere Web Client an, der mit dem vCenter Server-System mit Administratorrechten verbunden ist.

2 Klicken Sie auf **Regeln und Profile** und wählen Sie **Hostprofile** aus.

3 Klicken Sie auf das Symbol „Profil vom Host extrahieren“ und befolgen Sie die Aufforderungen des Assistenten.

Option	Beschreibung
Host auswählen	Wählen Sie den zuvor konfigurierten Referenzhost aus.
Name und Beschreibung	Benennen Sie das Profil „ESXiGold“ und fügen Sie ihm eine Beschreibung hinzu.
Bereit zum Abschließen	Überprüfen Sie die Informationen und klicken Sie auf **Beenden**.

4 Klicken Sie mit der rechten Maustaste auf das ESXiGold-Hostprofil und wählen Sie **Hosts und Cluster anhängen/trennen**.

5 Wählen Sie den ESXi-Host aus, an den Sie das Profil anhängen möchten, klicken Sie auf **Anhängen** und dann auf **Weiter**.

   Der Assistent lädt die Hostanpassung.

6 Geben Sie die Anpassungsinformationen ein und klicken Sie auf **Beenden**.

Weiter

Erstellen Sie eine Regel, die allen Hosts, die Sie mit Auto Deploy bereitstellen möchten, das Image-Profil und das neu erstellte Hostprofil zuweist. Weitere Informationen hierzu finden Sie unter „Erstellen einer Regel für andere Zielhosts“, auf Seite 147.

Erstellen einer Regel für andere Zielhosts

Sie können eine Regel erstellen, die das zuvor überprüfte Image-Profil und das soeben erstellte Hostprofil auf alle Zielhosts anwendet.

Bei dieser Aufgabe wird davon ausgegangen, dass Sie über grundlegende Kenntnisse der Microsoft PowerShell und vSphere PowerCLI verfügen.

Voraussetzungen

- Stellen Sie sicher, dass Ihr System die Anforderungen in der Vorinstallations-Checkliste erfüllt. Siehe „Checkliste für Machbarkeitsnachweis“, auf Seite 135.
- Führen Sie alle vorangegangenen Machbarkeitsnachweis-Setupaufgaben durch. Die vollständige Liste finden Sie unter „Machbarkeitsnachweis-Setup für Auto Deploy“, auf Seite 135.

Vorgehensweise

1 Melden Sie sich entweder direkt oder über RDP mit Administratorrechten bei der Konsole des Windows-Systems an, auf dem vCenter Server installiert ist.

2 Starten Sie eine PowerCLI-Sitzung und geben Sie die folgenden Befehle an der Eingabeaufforderung ein (drücken Sie die Eingabetaste nach jedem Befehl).

```
Connect-VIServer -Server your_vc_hostname -User username -Password password
Add-EsxSoftwareDepot path:\VMware-Esxi-version-xxxxx-depot.zip
```

   Geben Sie den vollständigen Pfad und den Dateinamen der ZIP-Datei an, die Sie zuvor heruntergeladen haben. Das Hinzufügen des Software-Depots ist bei jedem Start einer neuen PowerCLI-Sitzung erforderlich.

3 (Optional) Um die Regeln im aktiven Regelsatz anzuzeigen, geben Sie das folgende cmdlet an der Eingabeaufforderung ein und drücken Sie die Eingabetaste.

```
Get-DeployRuleset
```

4 Um eine Regel zu erstellen, die Auto Deploy anweist, die Hosts im angegebenen IP-Bereich mit dem von Ihnen ausgewählten Image und mit dem Hostprofil bereitzustellen, das Sie anhand des Referenzhosts erstellt haben, geben Sie den folgenden Befehl ein und drücken Sie die Eingabetaste.

```
New-DeployRule -name "Production01Rule" -item "Image-Pofile", ESXiGold,Zielcluster -Pattern "ipv4=IP-Bereich"
```

Option	Beschreibung
Image-Profil	Das ESXi-Image-Profil, das Sie in der ersten Bereitstellungsregel verwendet haben.
Zielcluster	Name des Clusters in vCenter Server, zu dem Sie alle Hosts hinzufügen möchten.
IP-Bereich	Geben Sie eine einzelne IP-Adresse oder einen Bereich von IP-Adressen für die Hosts an, die Sie anhand des Image-Profils und des Hostprofils bereitstellen möchten.

Wenn Sie einen Zielcluster angeben, wird das Hostprofil auf alle Hosts im Cluster angewendet. Es ist nicht erforderlich, das Hostprofil auf jeden Host anzuwenden.

5 Fügen Sie die neue Regel dem aktiven Regelsatz hinzu.

`Add-DeployRule -DeployRule "Production01Rule"` <Eingabetaste drücken>

6 (Optional) Entfernen Sie die Bereitstellungsregel, die Sie für den anfänglichen Startvorgang erstellt haben.

`Remove-DeployRule -DeployRule InitialBootRule` <Eingabetaste drücken>

7 Prüfen Sie den aktiven Regelsatz.

`Get-DeployRuleset`<Enter>

PowerCLI zeigt ähnliche Informationen wie im folgenden Beispiel an.

```
Name:           Production01Rule
PatternList:    {ipv4=address_range}
ItemList:       {ESXi-version-XXXXXX-standard, Compute01, ESXiGold}
```

Weiter

Stellen Sie alle Hosts bereit und richten Sie Hostanpassungen für jeden Host ein. Siehe „Bereitstellen aller Hosts und Einrichten von Hostanpassungen“, auf Seite 148.

Bereitstellen aller Hosts und Einrichten von Hostanpassungen

Mit der Regel zur Bereitstellung von Hosts mit einem Image-Profil und mit dem über den verfügbaren Referenzhost erstellten Hostprofil können Sie alle Zielhosts bereitstellen. Wenn bestimmte Hostprofilelemente so festgelegt sind, dass sie zur Benutzereingabe auffordern, wird der Host im Wartungsmodus ausgeführt. Sie wenden das Hostprofil an oder überprüfen die Hostübereinstimmung, die nach Informationen abgefragt wird. Das System verknüpft die Hostanpassung mit dem Host.

Voraussetzungen

- Stellen Sie sicher, dass Ihr System die Anforderungen in der Vorinstallations-Checkliste erfüllt. Siehe „Checkliste für Machbarkeitsnachweis“, auf Seite 135.
- Führen Sie alle vorangegangenen Machbarkeitsnachweis-Setupaufgaben durch. Die vollständige Liste finden Sie unter „Machbarkeitsnachweis-Setup für Auto Deploy“, auf Seite 135.
- Öffnen Sie eine Konsole für jeden Host, den Sie bereitstellen möchten, um den Fortschritt der Startvorgänge zu überwachen.

Vorgehensweise

1 Starten Sie die verbleibenden Hosts.

   Auto Deploy startet die Hosts, wendet das Hostprofil an und fügt die Hosts zur vCenter Server-Bestandsliste hinzu. Die Hosts verbleiben im Wartungsmodus, da das Hostprofil vom Referenzhost so eingerichtet ist, dass Benutzereingaben für jeden Host erforderlich sind.

2 Stellen Sie mit einem vSphere Web Client eine Verbindung mit dem vCenter Server-System her.

3 Klicken Sie auf **Home** und wählen Sie **Hostprofile**.

4 Wählen Sie im linken Fenster das ESXiGold-Profil aus und fügen Sie die neu gestarteten Hosts zu diesem Profil hinzu.

5 Wenden Sie das Hostprofil für jeden Host an, geben Sie die Benutzerinformationen ein und starten Sie jeden einzelnen Host neu.

   Nach Abschluss des Neustarts werden alle Hosts mit dem von Ihnen angegebenen Image ausgeführt und verwenden die Konfiguration im Referenzhostprofil. Der Cluster zeigt an, dass alle Hosts vollständig kompatibel sind.

Alle Hosts sind jetzt mit den über das Referenzhostprofil freigegeben Informationen und mit den hostspezifischen Informationen über den Mechanismus der Hostanpassung konfiguriert. Beim nächsten Starten der Hosts werden diese Informationen abgerufen und die Hosts werden vollständig gestartet.

Weiter

Nach erfolgreichem Abschluss der Beispielimplementierung können Sie mit der Planung des Produktions-Setups beginnen.

Verwenden von vSphere ESXi Image Builder

vSphere ESXi Image Builder ist ein Satz von vSphere PowerCLI-Cmdlets, die Sie zum Verwalten von vSphere-Image-Profilen und VIB-Paketen, wie z. B. Treiber-VIBs und Update-VIBs, verwenden können. Sie können mit vSphere ESXi Image Builder-Cmdlets auch ein Image-Profil in eine ISO- oder Offline-Depot-ZIP-Datei exportieren, die Sie zum Installieren von ESXi mit einem benutzerdefinierten Satz von Updates, Patches und Treibern verwenden können.

Grundlegende Informationen zu vSphere ESXi Image Builder

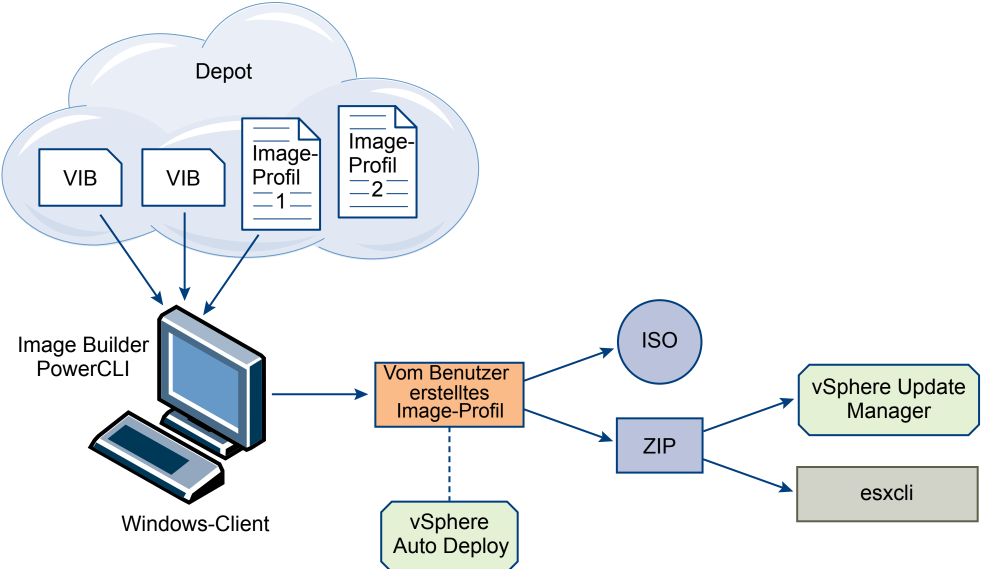
Mit VMware vSphere® ESXi™ Image Builder CLI können Sie Softwaredepots, Image-Profile und Softwarepakete (VIBs) verwalten. Image-Profile und VIBs spezifizieren die Software, die Sie während der Installation oder des Upgrades eines ESXi-Host verwenden möchten.

Überblick über vSphere ESXi Image Builder

Mit vSphere ESXi Image Builder können Sie vSphere-Image-Profile und VIBs verwalten.

VIBs sind Softwarepakete, und Image-Profile enthalten einen Satz von Softwarepaketen. Siehe „Software-Depots und ihre Komponenten“, auf Seite 151.

Abbildung 4-6. Image Builder-Architektur



Sie verwenden vSphere ESXi Image Builder-cmdlets zum Verwalten der Software, die auf Ihren ESXi-Hosts bereitgestellt werden soll, in verschiedenen Situationen.

Tabelle 4-14. Fälle, in denen Sie vSphere ESXi Image Builder verwenden können

Anwendungsfall für vSphere ESXi Image Builder	Beschreibung
Erstellen von Image-Profilen zur Verwendung durch vSphere Auto Deploy	Verwenden Sie vSphere ESXi Image Builder zum Erstellen eines Image-Profils, das die VIBs definiert, die vSphere Auto Deploy zum Bereitstellen von Hosts verwendet.
Fügen Sie benutzerdefinierte Drittanbieter-Treiber zu einem vorhandenen Image-Profil hinzu und exportieren Sie es in eine ISO-Datei oder in ein Paket	Wenn Sie benutzerdefinierte VIBs für Drittanbieter-Treiber oder -Erweiterungen zu Ihren ESXi-Hosts hinzufügen, verwenden Sie vSphere ESXi Image Builder, um das von VMware bereitgestellte Basis-Image zu klonen, fügen Sie die benutzerdefinierten VIBs hinzu und exportieren Sie es in eine ISO-Datei oder in eine Offline-Paket-ZIP-Datei.
Upgrades durchführen	Wenn Sie ein Upgrade von einem System der Version 4.0 oder 4.1 durchführen, das benutzerdefinierte Erweiterungen oder Treiber enthält, können Sie vSphere ESXi Image Builder verwenden, um ein Image-Profil zu erstellen, das das vSphere 5-Basis-VIB enthält. Sie können vSphere 5 VIBs für die benutzerdefinierten Erweiterungen und diese VIBs dem Basis-VIB hinzufügen. Exportieren Sie das benutzerdefinierte Image-Profil in ein ISO, das Sie installieren können, oder in eine ZIP-Datei, die Sie mit vSphere Update Manager verwenden können.
Erstellen benutzerdefinierter Images mit einem geringeren Speicherplatzbedarf	Wenn Sie ein Image mit minimalem Speicherplatzbedarf benötigen, können Sie das ESXi-Basis-Image-Profil klonen und VIBs mithilfe des vSphere ESXi Image Builder entfernen.

Die vSphere ESXi Image Builder-cmdlets nehmen Image-Profile und VIBs als Eingabe und erzeugen verschiedene Ausgaben.

Tabelle 4-15. Eingabe und Ausgabe bei den vSphere ESXi Image Builder-cmdlets

Parameter	Beschreibung
Eingabe	Image-Profile und VIBs, die sich in einem Software-Depot befinden, werden als Eingabe für vSphere PowerCLI-cmdlets verwendet, die auf einem Windows-Client ausgeführt werden.
Ausgabe	vSphere PowerCLI-cmdlets erstellen benutzerdefinierte Image-Profile, die in ein ISO-Image oder in eine Offline-Depot-ZIP-Datei exportiert werden können. ISO-Images werden zur Installation verwendet. Das ZIP-Depot kann von Update Manager oder `esxcli software`-Befehlen verwendet werden, um Images zu aktualisieren oder zu installieren. Image-Profile werden außerdem in vSphere Auto Deploy-Regeln verwendet, um die Software anzupassen, mit der ESXi-Hosts bereitgestellt werden sollen.

Im Video „Using Image Builder CLI (Verwendung von Image Builder CLI)“ erhalten Sie Informationen zu vSphere ESXi Image Builder:



Using Image Builder CLI (Verwendung von Image Builder CLI) (http://link.brightcove.com/services/player/bcpid2296383276001?bctid=ref:video_using_image_builder_cli)

Software-Depots und ihre Komponenten

Das Verständnis, wie Depots, Profile und VIBs strukturiert sind und wo Sie sie verwenden können, ist Voraussetzung für die Installation eines benutzerdefinierten ESXi-ISO im Arbeitsspeicher, für die Bereitstellung von ESXi-Hosts mithilfe von vSphere Auto Deploy und für bestimmte benutzerdefinierte Upgrade-Vorgänge.

Die folgenden technischen Begriffe werden in der vSphere-Dokumentation im Zusammenhang mit Installations- und Upgrade-Aufgaben verwendet.

VIB

Ein VIB ist ein ESXi-Software-Paket. Paketlösungen, Treiber, CIM-Anbieter und Anwendungen von VMware und seinen Partnern, die die ESXi-Plattform als VIBs erweitern. VIBs sind in Software-Depots verfügbar. Sie können VIBs zur Erstellung und Anpassung von ISO-Images oder zum Upgrade von ESXi-Hosts verwenden, indem Sie VIBs asynchron auf den Hosts installieren.

Siehe „SoftwarePackage-Objekteigenschaften“, auf Seite 155.

Image-Profil

Ein Image-Profil definiert ein ESXi-Image und besteht aus VIBs. Ein Image-Profil enthält immer ein Basis-VIB und umfasst möglicherweise weitere VIBs. Image-Profile werden mithilfe von vSphere ESXi Image Builder untersucht und definiert.

Siehe „ImageProfile-Objekteigenschaften“, auf Seite 155.

Software-Depot

Ein Software-Depot ist eine Sammlung von VIBs und Image-Profilen. Das Software-Depot ist eine Hierarchie von Dateien und Ordnern und es kann über eine HTTP-URL (Online-Depot) oder eine ZIP-Datei (Offline-Depot) bereitgestellt werden. VMware und VMware-Partner stellen Depots bereit. Unternehmen mit großen VMware-Installationen erstellen möglicherweise interne Depots, um ESXi-Hosts mit vSphere Auto Deploy bereitzustellen oder um eine ISO-Datei für die ESXi-Installation zu exportieren.

Überblick über vSphere ESXi Image Builder-Cmdlets

vSphere ESXi Image Builder-Cmdlets ermöglichen Ihnen das Verwalten von Image-Profilen und VIBs.

vSphere ESXi Image Builder enthält die folgenden Cmdlets.

Hinweis Geben Sie bei der Ausführung von vSphere ESXi Image Builder-Cmdlets alle Parameter in der Befehlszeile an, wenn Sie das Cmdlet aufrufen. Die Angabe von Parametern im interaktiven Modus wird nicht empfohlen.

Führen Sie `Get-Help` *Cmdlet-Name* an der vSphere PowerCLI-Eingabeaufforderung aus, um detaillierte Referenzinformationen zu erhalten.

Tabelle 4-16. vSphere ESXi Image Builder-Cmdlets

Cmdlet	Beschreibung
`Add-EsxSoftwareDepot`	Fügt das Softwaredepot oder die ZIP-Datei am angegebenen Speicherort zu Ihrer aktuellen Umgebung hinzu. Lädt Metadaten aus dem Depot herunter und analysiert VIBs auf Abhängigkeiten.
`Remove-EsxSoftwareDepot`	Trennt die Verbindung zum angegebenen Softwaredepot.
`Get-EsxSoftwareDepot`	Gibt eine Liste der Software-Depots zurück, die sich in der aktuellen Umgebung befinden. Wenn Sie die Image-Profile und VIBs untersuchen und verwalten möchten, müssen Sie zuerst das entsprechende Software-Depot in Ihrer Umgebung hinzufügen.
`Get-EsxSoftwarePackage`	Gibt eine Liste von Softwarepaket-Objekten (VIBs) zurück. Verwenden Sie die Optionen dieses cmdlets zum Filtern der Ergebnisse.
`Get-EsxImageProfile`	Gibt ein Array von `ImageProfile`-Objekten aus allen momentan hinzugefügten Depots zurück.
`New-EsxImageProfile`	Erstellt ein neues Image-Profil. In den meisten Fällen wird empfohlen, ein neues Profil durch das Klonen eines vorhandenen Profils zu erstellen. Siehe „Klonen eines Image-Profils“, auf Seite 160.
`Set-EsxImageProfile`	Ändert ein lokales `ImageProfile`-Objekt und führt Validierungstests für das geänderte Profil durch. Das cmdlet gibt das geänderte Objekt zurück, behält es jedoch nicht bei.
`Export-EsxImageProfile`	Exportiert ein Image-Profil entweder als ESXi-ISO-Image für die ESXi-Installation oder als ZIP-Datei.
`Compare-EsxImageProfile`	Gibt eine `ImageProfileDiff`-Struktur zurück, die zeigt, ob die beiden Profile dieselbe VIB-Liste und Akzeptanzebene haben. Siehe „Akzeptanzebenen“, auf Seite 154.
`Remove-EsxImageProfile`	Entfernt das Image-Profil aus dem Software-Depot.
`Add-EsxSoftwarePackage`	Fügt ein oder mehrere neue Pakete (VIBs) zu einem vorhandenen Image-Profil hinzu.
`Remove-EsxSoftwarePackage`	Entfernt ein oder mehrere Pakete (VIBs) aus einem Image-Profil.

Image-Profile

Image-Profile definieren die VIBs, die ein Installations- oder Update-Prozess von ESXi verwendet. Image-Profile gelten für Hosts, die mit vSphere Auto Deploy bereitgestellt wurden, und für andere ESXi 5.x-Hosts. Sie definieren und manipulieren Image-Profile mit vSphere ESXi Image Builder.

Anforderungen an Image-Profils

Sie können ein benutzerdefiniertes Image-Profil von Grund auf neu erstellen oder ein vorhandenes Profil klonen und VIBs hinzufügen oder entfernen. Ein Profil muss die folgenden Anforderungen erfüllen, um gültig zu sein.

- Jedes Image-Profil muss eine eindeutige Kombination aus Name und Anbieter haben.
- Jedes Image-Profil hat eine Akzeptanzebene. Wenn Sie ein VIB mithilfe eines vSphere ESXi Image Builder-Cmdlets zu einem Image-Profil hinzufügen, überprüft Image Builder, ob das VIB der für das Profil definierten Akzeptanzebene entspricht.
- Sie können keine VIBs entfernen, die von anderen VIBs benötigt werden.
- Sie können nicht zwei Versionen desselben VIBs zu einem Image-Profil hinzufügen. Wenn Sie eine neue Version eines VIBs hinzufügen, ersetzt die neue Version die vorhandene Version des VIBs.

Image-Profil-Validierung

Ein Image-Profil und dessen VIBs müssen verschiedene Kriterien erfüllen, um gültig zu sein.

- Image-Profile müssen mindestens ein Basis-VIB und ein startfähiges Kernelmodul enthalten.
- Wenn ein VIB im Image-Profil von einem anderen VIB abhängig ist, muss dieses andere VIB auch im Image-Profil enthalten sein. VIB-Ersteller speichern diese Informationen in der Eigenschaft „Depends“ des SoftwarePackage-Objekts.
- VIBs dürfen nicht miteinander in Konflikt stehen. VIB-Ersteller speichern Informationen zu Konflikten in der Eigenschaft „Conflicts“ des SoftwarePackage-Objekts.
- Es können nicht zwei VIBs mit demselben Namen, aber unterschiedlichen Versionen, nebeneinander vorhanden sein. Wenn Sie eine neue Version eines VIBs hinzufügen, ersetzt die neue Version die vorhandene Version des VIBs.
- Es bestehen keine Probleme hinsichtlich der Validierung der Akzeptanzebene.

Wenn Sie eine Änderung an einem Image-Profil vornehmen, überprüft vSphere ESXi Image Builder, ob die Änderung das Profil ungültig macht.

Validierung von Abhängigkeiten

Wenn Sie ein VIB hinzufügen oder entfernen, überprüft vSphere ESXi Image Builder, ob Paketabhängigkeiten eingehalten werden. Jedes SoftwarePackage-Objekt enthält eine „Depends“-Eigenschaft, die eine Liste anderer VIBs angibt, von denen dieses VIB abhängig ist. Siehe „Struktur der ImageProfile-, SoftwarePackage- und ImageProfileDiff-Objekte“, auf Seite 155.

Akzeptanzebenen-Validierung

vSphere ESXi Image Builder führt jedes Mal, wenn ein Image-Profil erstellt oder geändert wird, eine Validierung der Akzeptanzebene durch. vSphere ESXi Image Builder prüft die Akzeptanzebene von VIBs im Image-Profil im Vergleich zu der mindestens zulässigen Akzeptanzebene des Profils. Die Akzeptanzebene des VIBs wird darüber hinaus jedes Mal validiert, wenn die Signatur eines VIBs validiert wird.

VIB-Validierung während des Exports

Wenn Sie ein Image-Profil in ein ISO exportieren, validiert vSphere ESXi Image Builder jedes VIB, indem die folgenden Aktionen ausgeführt werden.

- Überprüft, ob Konflikte bestehen, indem die Eigenschaft „Conflicts" der einzelnen SoftwarePackage-Objekte geprüft wird.
- Führt die VIB-Signaturvalidierung durch. Die Signaturvalidierung verhindert das unbefugte Ändern von VIB-Paketen. Die Signatur ist eine kryptographische Prüfsumme, die garantiert, dass ein VIB von seinem Autor erzeugt wurde. Die Signaturvalidierung findet auch während der Installation von VIBs auf einem ESXi-Host und bei der Verwendung von VIBs durch den vSphere Auto Deploy-Server statt.
- Überprüft, ob die VIBs die Dateipfad-Verwendungsregeln einhalten. VMware testet VMwareCertified- und VMwareAccepted-VIBs, um zu garantieren, dass diese VIBs immer den Dateipfad-Nutzungsregeln entsprechen.

Akzeptanzebenen

Jedes VIB wird mit einer Akzeptanzebene freigegeben, die nicht geändert werden kann. Die Akzeptanzebene des Hosts bestimmt, welche VIBs auf einem Host installiert werden dürfen. Sie können mithilfe der `esxcli`-Befehle die Host-Akzeptanzebenen ändern.

VMware unterstützt die folgenden Akzeptanzebenen.

VMwareCertified
Die Akzeptanzebene „VMwareCertified" hat die strengsten Anforderungen. VIBs dieser Ebene unterliegen einer gründlichen Prüfung entsprechend den internen VMware-Qualitätssicherungstests für die gleiche Technologie. Heute werden nur IOVP-Treiber auf dieser Ebene veröffentlicht. VMware übernimmt Support-Anrufe für VIBs dieser Akzeptanzebene.

VMwareAccepted
VIBs dieser Akzeptanzebene unterliegen einer Verifizierungsprüfung; es wird jedoch nicht jede Funktion der Software in vollem Umfang getestet. Der Partner führt die Tests durch und VMware verifiziert das Ergebnis. Heute gehören CIM-Anbieter und PSA-Plug-Ins zu den VIBs, die auf dieser Ebene veröffentlicht werden. VMware leitet Support-Anrufe für VIBs dieser Akzeptanzebene an die Support-Organisation des Partners weiter.

PartnerSupported
VIBs mit der Akzeptanzebene „PartnerSupported" werden von einem Partner veröffentlicht, dem VMware vertraut. Der Partner führt alle Tests durch. VMware überprüft die Ergebnisse nicht. Diese Ebene wird für eine neue oder nicht etablierte Technologie verwendet, die Partner für VMware-Systeme aktivieren möchten. Auf dieser Ebene sind heute Treiber-VIB-Technologien mit nicht standardisierten Hardwaretreibern, wie z. B. Infiniband, ATAoE und SSD. VMware leitet Support-Anrufe für VIBs dieser Akzeptanzebene an die Support-Organisation des Partners weiter.

CommunitySupported
Die Akzeptanzebene „CommunitySupported" ist für VIBs gedacht, die von Einzelpersonen oder Unternehmen außerhalb der VMware Partner-Programme erstellt wurden. VIBs auf dieser Ebene wurden nicht im Rahmen eines von VMware zugelassenen Testprogramms getestet und werden weder von VMware Technical Support noch von einem VMware-Partner unterstützt.

Struktur der ImageProfile-, SoftwarePackage- und ImageProfileDiff-Objekte

Die Kenntnis der Struktur der Objekte `ImageProfile`, `SoftwarePackage` und `ImageProfileDiff` hilft bei der Verwaltung von Bereitstellungen und Upgrades.

ImageProfile-Objekteigenschaften

Das Objekt `ImageProfile`, auf das über das vSphere PowerCLI-Cmdlet `Get-EsxImageProfile` zugegriffen werden kann, weist die folgenden Eigenschaften auf.

Name	Typ	Beschreibung
`AcceptanceLevel`	`AcceptanceLevel`	Legt fest, welche VIBs Sie zu dem Profil hinzufügen können. Mögliche Ebenen sind VMwareCertified, VMwareAccepted, PartnerSupported und CommunitySupported. Siehe „Akzeptanzebenen“, auf Seite 154.
`Autor`	`System.String`	Die Person, die das Profil erstellt hat. 60 Zeichen oder weniger.
`CreationTime`	`System.DateTime`	Der Zeitstempel der Erstellungszeit
`Beschreibung`	`System.String`	Die Volltextbeschreibung des Profils. Keine Längenbeschränkung.
`GUID`	`System.String`	Globale eindeutige ID des Image-Profils.
`ModifiedTime`	`System.DateTime`	Der Zeitstempel der letzten Änderung
`Name`	`System.String`	Der Name des Image-Profils. 80 Zeichen oder weniger.
`ReadOnly`	`System.Boolean`	Wenn auf `true` gesetzt, kann das Profil nicht bearbeitet werden. Verwenden Sie `Set-EsxImageProfile -Readonly`, um Ihre benutzerdefinierten Image-Profile nur zum Lesen freizugeben.
`Regeln`	`ImageProfileRule[]`	Alle OEM-Hardwareanforderungen und -einschränkungen, die das Image-Profil möglicherweise aufweist. vSphere Auto Deploy überprüft den Wert dieser Eigenschaft, wenn es ein Image-Profil bereitstellt, und stellt das Profil bereit, wenn passende Hardware verfügbar ist.
`Anbieter`	`System.String`	Die Organisation, die das Profil veröffentlicht. 40 Zeichen oder weniger.
`VibList`	`SoftwarePackage[]`	Eine Liste der VIB-IDs, aus denen das Image besteht

SoftwarePackage-Objekteigenschaften

Wenn Sie ein Image-Profil vorbereiten, können Sie Softwarepakete untersuchen, um zu entscheiden, welche Pakete zur Einbeziehung geeignet sind. Das `SoftwarePackage`-Objekt hat folgende Eigenschaften.

Name	Typ	Beschreibung
`AcceptanceLevel`	`AcceptanceLevel`	Die Akzeptanzebene dieses VIB
`Konflikte`	`SoftwareConstraint[]`	Eine Liste der VIBs, die nicht gleichzeitig mit diesem VIB installiert werden können. Jede Einschränkung hat das folgende Format: `Paketname[<<|<=|=|>=|<< Version]`
`Depends`	`SoftwareConstraint[]`	Eine Liste der VIBs, die gleichzeitig mit diesem VIB installiert sein müssen. Gleiches Einschränkungsformat wie die `Conflicts`-Eigenschaft.
`Beschreibung`	`System.String`	Die ausführliche Beschreibung des VIB
`GUID`	`System.String`	Die eindeutige ID des VIB
`LiveInstallOk`	`System.Boolean`	„True“, wenn Live-Installationen dieses VIB unterstützt werden.
`LiveRemoveOk`	`System.Boolean`	„True“, wenn Live-Entfernungen dieses VIB unterstützt werden.
`MaintenanceMode`	`System.Boolean`	„True“, wenn sich Hosts bei Installation dieses VIB im Wartungsmodus befinden müssen.
`Name`	`System.String`	Der Name des VIB. Beschreibt in der Regel das Paket auf einem laufenden ESXi-System eindeutig.
`Provides`	`SoftwareProvides`	Die Liste der virtuellen Pakete oder Schnittstellen, die dieses VIB bereitstellt. Siehe „SoftwareProvide-Objekteigenschaften“, auf Seite 158.
`ReferenceURLs`	`SupportReference[]`	Die Liste von `SupportReference`-Objekten mit umfassenden Supportinformationen. Das `SupportReference`-Objekt weist zwei Eigenschaften auf, `Title` und `URL`, beide des Typs `System.String`.
`Replaces`	`SoftwareConstraint[]`	Die Liste von `SoftwareConstraint`-Objekten, die VIBs identifizieren, die dieses VIB replizieren oder es obsolet machen. VIBs ersetzen automatisch VIBs mit demselben Namen, die niedrigere Versionen aufweisen.
`ReleaseDate`	`System.DateTime`	Datum und Uhrzeit der VIB-Veröffentlichung oder -Freigabe.
`SourceUrls`	`System.String[]`	Die Liste der Quell-URLs, von denen dieses VIB heruntergeladen werden kann
`StatelessReady`	`System.Boolean`	„True“, wenn das Paket Hostprofile oder andere Technologien unterstützt, die es für die Verwendung im Zusammenhang mit vSphere Auto Deploy geeignet machen.
`Übersicht`	`System.String`	Eine einzeilige Zusammenfassung des VIB

Name	Typ	Beschreibung
Tags	System.String[]	Ein Array von Zeichenketten-Tags für dieses Paket, das vom Hersteller oder Herausgeber definiert wird. Tags können für die Ermittlung der Eigenschaften eines Pakets verwendet werden.
Anbieter	System.String	Der VIB-Anbieter oder -Herausgeber
Version	System.String	Die VIB-Version
VersionObject	Software.Version	Die VersionObject-Eigenschaft ist vom Typ SoftwareVersion. Die SoftwareVersion-Klasse implementiert eine statische Compare-Methode, um zwei Zeichenfolgenversionen zu vergleichen. Siehe „SoftwareVersion-Objekteigenschaften", auf Seite 158.

ImageProfileDiff-Objekteigenschaften

Wenn Sie das Compare-EsxImageProfile-cmdlet ausführen, übergeben Sie zwei Parameter, zuerst das Referenzprofil und dann das Vergleichsprofil. Das cmdlet gibt ein ImageProfileDiff-Objekt zurück, das folgende Eigenschaften hat.

Name	Typ	Beschreibung
CompAcceptanceLevel	System.String	Die Akzeptanzebene des zweiten Profils, das Sie an Compare-EsxImageProfile übergeben haben
DowngradeFromRef	System.String[]	Die Liste der VIBs im zweiten Profil, bei denen es sich um Herabstufungen von VIBs des ersten Profils handelt
Equal	System.Boolean	True, wenn die beiden Image-Profile über die gleichen Pakete und Akzeptanzebenen verfügen
OnlyInComp	System.String	Die Liste der VIBs, die nur im zweiten Profil gefunden wurden, das Sie an Compare-EsxImageProfile übergeben haben
OnlyInRef	System.String[]	Die Liste der VIBs, die nur im ersten Profil gefunden wurden, das Sie an Compare-EsxImageProfile übergeben haben
PackagesEqual	System.Boolean	True, wenn die Image-Profile über die gleichen VIB-Pakete verfügen.
RefAcceptanceLevel	System.String	Die Akzeptanzebene des ersten Profils, das Sie an Compare-EsxImageProfile übergeben haben
UpgradeFromRef	System.String[]	Die Liste der VIBs im zweiten Profil, bei denen es sich um Upgrades von VIBs des ersten Profils handelt

SoftwareVersion-Objekteigenschaften

Mit dem Objekt SoftwareVersion können Sie zwei Versionszeichenfolgen vergleichen. Das Objekt enthält eine statische Compare-Methode, die zwei Zeichenfolgen als Eingabe übernimmt und 1 zurückgibt, wenn die erste Versionszeichenfolge höher als die zweite Versionszeichenfolge ist. Compare gibt 0 zurück, wenn zwei Versionszeichenfolgen gleich sind. Compare gibt -1 zurück, wenn die zweite Versionszeichenfolge höher ist als die erste. Das Objekt hat folgende Eigenschaften.

Name	Typ	Beschreibung
Version	System.String	Der Teil der Version vor dem Bindestrich. Dieser Teil zeigt die Hauptversion.
Version	System.String	Der Teil der Version nach dem Bindestrich. Dieser Teil zeigt die Release-Version.

SoftwareConstraint-Objekteigenschaften

Das SoftwareConstraint-Objekt implementiert eine MatchesProvide-Methode. Die Methode akzeptiert ein SoftwareProvides- oder SoftwarePackage-Objekt als Eingabe und gibt True zurück, wenn die Einschränkung mit SoftwareProvide oder SoftwarePackage übereinstimmt, und False in allen anderen Fällen.

Das Objekt SoftwareConstraint weist die folgenden Eigenschaften auf.

Name	Typ	Beschreibung
Name	System.String	Der Name der Einschränkung. Dieser Name muss mit einer entsprechenden Eigenschaft SoftwareProvide Name übereinstimmen.
Relation	System.String	Ein enum-Objekt oder einer der folgenden Vergleichsindikatoren: <<, <=, = >=, >>. Diese Eigenschaft kann $null sein, wenn die Einschränkung keine Relation- und Version-Eigenschaft hat.
Version	System.String	Die Version, mit der die Einschränkung übereinstimmen soll. Diese Eigenschaft kann $null sein, wenn die Einschränkung keine Relation- und Version-Eigenschaft hat.
VersionObject	SoftwareVersion	Die Version, die durch ein SoftwareVersion-Objekt repräsentiert wird.

SoftwareProvide-Objekteigenschaften

Das SoftwareProvide-Objekt hat folgende Eigenschaften.

Name	Typ	Beschreibung
Name	System.String	Der Name des provide-Objekts
Version	System.String	Die Version des provide-Objekts. Kann $null sein, wenn das provide-Objekt keine Version angibt.
Version	System.String	Die Version des provide-Objekts in der Darstellung durch ein SoftwareVersion-Objekt. Siehe „SoftwareVersion-Objekteigenschaften“, auf Seite 158.

Installation und Verwendung von vSphere ESXi Image Builder

vSphere ESXi Image Builder besteht aus dem vSphere ESXi Image Builder-Server und den vSphere ESXi Image Builder PowerShell-Cmdlets. Der vSphere ESXi Image Builder-Server wird gestartet, wenn Sie das erste vSphere ESXi Image Builder-Cmdlet ausführen.

Installieren von vSphere ESXi Image Builder und erforderlicher Software

Bevor Sie vSphere ESXi Image Builder-cmdlets ausführen können, müssen Sie vSphere PowerCLI und die erforderliche Software installieren. Das vSphere ESXi Image Builder-Snap-In ist im Lieferumfang der vSphere PowerCLI-Installation enthalten.

Sie installieren vSphere ESXi Image Builder und die erforderliche Software auf einem Microsoft Windows-System.

Vorgehensweise

1 Installieren Sie Microsoft .NET 2.0 von der Microsoft-Website aus gemäß den Anweisungen auf dieser Website.

2 Installieren Sie Microsoft PowerShell 2.0 von der Microsoft-Website aus gemäß den Anweisungen auf dieser Website.

3 Installieren Sie vSphere PowerCLI, in der die vSphere ESXi Image Builder-cmdlets enthalten sind.

   Genauere Anweisungen finden Sie im *vSphere PowerCLI-Installationshandbuch*.

Weiter

Lesen Sie „Verwenden von vSphere ESXi Image Builder-cmdlets“, auf Seite 159. Wenn Sie vSphere PowerCLI noch nicht benutzt haben, lesen Sie die Dokumentation zu vSphere PowerCLI.

Verwenden Sie vSphere ESXi Image Builder-cmdlets sowie andere vSphere PowerCLI- und PowerShell-cmdlets zum Verwalten von Image-Profilen und VIBs. Sie können mithilfe von `Get-Help` *Name_des_cmdlets* jederzeit Hilfe aufrufen.

Verwenden von vSphere ESXi Image Builder-cmdlets

vSphere ESXi Image Builder-cmdlets werden als Microsoft PowerShell-cmdlets implementiert und sind in vSphere PowerCLI enthalten. Benutzer von vSphere ESXi Image Builder-cmdlets haben den Vorteil, alle vSphere PowerCLI-Funktionen nutzen zu können.

Erfahrene PowerShell-Benutzer können vSphere ESXi Image Builder-cmdlets genau wie andere PowerShell-cmdlets verwenden. Wenn Sie PowerShell und vSphere PowerCLI erst seit Kurzem verwenden, sollten Sie die folgenden Tipps nutzen.

Sie können cmdlets, Parameter und Parameterwerte in die vSphere PowerCLI-Shell eingeben.

- Sie erhalten Hilfe zu jedem cmdlet , indem Sie `Get-Help` *`Name_des_cmdlets`* ausführen.
- Beachten Sie, dass bei PowerShell die Groß-/Kleinschreibung nicht beachtet wird.
- Verwenden Sie die Tabulatortaste zum Vervollständigen der cmdlet- und Parameternamen.
- Formatieren Sie die Ausgabe von Variablen und cmdlets mit `Format-List` oder `Format-Table` bzw. mit deren Kurzformen `fl` oder `ft`. Hilfe erhalten Sie, indem Sie `Get-Help Format-List` eingeben.
- Verwenden Sie Platzhalter zum Durchsuchen und Filtern von VIBs und Image-Profilen. Alle Platzhalterausdrücke werden unterstützt.

Übergeben von Parametern per Name

Sie können in den meisten Fällen Parameter per Name übergeben und Parameterwerte, die Leer- oder Sonderzeichen enthalten, in doppelte Anführungszeichen einschließen.

```
Add-EsxSoftwarePackage -ImageProfile profile42 -SoftwarePackage "partner package 35"
```

Übergeben von Parametern als Objekte

Sie können Parameter als Objekte übergeben, wenn Sie Scripting und Automatisierung verwenden. Sie können die Technik mit cmdlets verwenden, die mehrere Objekte zurückgeben, als auch mit cmdlets, die ein einzelnes Objekt zurückgeben.

1 Binden Sie die Ausgabe eines cmdlets, das mehrere Objekte zurückgibt, an eine Variable.

   ```
   $profs = Get-EsxImageProfile
   ```

2 Wann Sie das cmdlet ausführen, das das Objekt als Eingabe benötigt, greifen Sie per Position auf das Objekt zu, wobei die Liste mit 0 beginnt.

   ```
   Add-EsxSoftwarePackage -ImageProfile $profs[4] -SoftwarePackage partner-pkg
   ```

Im Beispiel wird das angegebene Softwarepaket zum fünften Image-Profil in der Liste, die von `Get-EsxImageProfile` zurückgegeben wird, hinzugefügt.

In den meisten Beispielen in der Dokumentation *Installations- und Einrichtungshandbuch für vSphere* werden die Parameter per Name übergeben. „vSphere ESXi Image Builder-Workflows“, auf Seite 169 enthält Beispiele, in denen Parameter als Objekte übergeben werden.

Allgemeine Aufgaben in vSphere ESXi Image Builder

Mit den Cmdlets in vSphere ESXi Image Builder können Sie Software-Depots, Image-Profile und VIBs bearbeiten.

Klonen eines Image-Profils

Das Klonen eines veröffentlichten Profils stellt die einfachste Möglichkeit zum Erstellen eines benutzerdefinierten Image-Profils dar. Das Klonen eines Profils ist besonders nützlich, wenn Sie einige VIBs aus einem Profil entfernen möchten, oder wenn Sie Hosts verschiedener Anbieter verwenden und dasselbe Basisprofil verwenden möchten, jedoch anbieterspezifische VIBs hinzugefügt werden sollen. Für VMware-Partner oder in umfangreichen Installationen kann es vorteilhaft sein, ein Profil neu zu erstellen.

Voraussetzungen

- Installieren Sie vSphere PowerCLI und alle erforderliche Software. Siehe „Installation und Verwendung von vSphere ESXi Image Builder“, auf Seite 159.
- Stellen Sie sicher, dass Sie Zugriff auf das Software-Depot haben, das das Image-Profil enthält, das Sie klonen möchten.

Vorgehensweise

1 Führen Sie in einer vSphere PowerCLI-Sitzung das Cmdlet `Add-EsxSoftwareDepot` für jedes Depot aus, mit dem Sie arbeiten möchten.

Option	Aktion
Remote-Depot	Führen Sie `Add-EsxSoftwareDepot -DepotUrl` *`URL_des_Depots`* aus.
ZIP-Datei	a Laden Sie die ZIP-Datei auf ein lokales Dateisystem herunter. b Führen Sie `Add-EsxSoftwareDepot -DepotUrl C:\Datei-pfad\`*`Offline-Paket`*`.zip` aus.

   Das Cmdlet gibt mindestens ein `SoftwareDepot`-Objekt zurück.

2 (Optional) Führen Sie das cmdlet `Get-EsxImageProfile` aus, um den Namen des zu klonenden Profils zu finden.

   Sie können Filteroptionen mit `Get-EsxImageProfile` verwenden.

3 Führen Sie das Cmdlet `New-EsxImageProfile` aus, um das neue Profil zu erstellen, und geben Sie mit dem Parameter `-CloneProfile` das zu klonende Profil an.

```
New-EsxImageProfile -CloneProfile My_Profile -Name "Test Profile 42"
```

   In diesem Beispiel wird das Profil *My_Profile* geklont und ihm der Name „Test Profil 42“ zugewiesen. Sie müssen für das geklonte Profil eine eindeutige Kombination aus Namen und Anbieter angeben.

Weiter

Unter „Untersuchen von Depot-Inhalten“, auf Seite 169 finden Sie Beispiele für das Filtern.

Passen Sie das Image-Profil an, indem Sie VIBs hinzufügen oder entfernen. Siehe „VIBs zu einem Image-Profil hinzufügen“, auf Seite 161.

VIBs zu einem Image-Profil hinzufügen

Sie können einem Image-Profil ein oder mehrere VIBs hinzufügen, wenn das Image-Profil nicht auf „read only“ gesetzt ist. Wenn das neue VIB von anderen VIBs abhängt oder mit anderen VIBs im Profil in Konflikt steht, wird eine Meldung an der PowerShell-Eingabeaufforderung angezeigt und das VIB wird nicht hinzugefügt.

Sie können einem Image-Profil VIBs von VMware oder von VMware-Partnern hinzufügen. Wenn Sie VMware-VIBs hinzufügen, führt vSphere ESXi Image Builder eine Validierung durch. Wenn Sie VIBs von zwei oder mehr OEM-Partnern gleichzeitig hinzufügen, werden zwar keine Fehler gemeldet, aber das resultierende Image-Profil funktioniert möglicherweise nicht. Installieren Sie VIBs jeweils nur von einem OEM-Anbieter.

Wenn ein Fehler zu Problemen mit der Akzeptanzebene angezeigt wird, ändern Sie die Akzeptanzebene des Image-Profils und die Akzeptanzebene des Hosts. Überlegen Sie genau, ob die Änderung der Host-Akzeptanzebene ratsam ist. VIB-Akzeptanzebenen werden während der Erstellung eines VIBs festgelegt und können nicht geändert werden.

Sie können VIBs hinzufügen, selbst wenn das resultierende Image-Profil ungültig ist.

Hinweis VMware kann nur Umgebungen und Konfigurationen unterstützen, deren Stabilität und volle Funktionsfähigkeit durch strenge und umfassende Tests erwiesen ist. Verwenden Sie nur diese unterstützten Konfigurationen. Sie können benutzerdefinierte VIBs verwenden, wenn Sie die Host-Akzeptanzebene und somit die Unterstützbarkeit senken. Verfolgen Sie in diesem Fall die vorgenommenen Änderungen, damit Sie sie später rückgängig machen können, wenn Sie die benutzerdefinierten VIBs entfernen und die Host-Akzeptanzebene auf den Standard (Partner Supporter) zurücksetzen möchten. Siehe „Arbeiten mit Akzeptanzebenen“, auf Seite 166.

Voraussetzungen

Installieren Sie vSphere PowerCLI und alle erforderliche Software. Siehe „Installieren von vSphere ESXi Image Builder und erforderlicher Software“, auf Seite 159.

Vorgehensweise

1. Führen Sie in einer vSphere PowerCLI-Sitzung das Cmdlet `Add-EsxSoftwareDepot` für jedes Depot aus, mit dem Sie arbeiten möchten.

Option	Aktion
Remote-Depot	Führen Sie `Add-EsxSoftwareDepot -DepotUrl` *`URL_des_Depots`* aus.
ZIP-Datei	a Laden Sie die ZIP-Datei auf ein lokales Dateisystem herunter. b Führen Sie `Add-EsxSoftwareDepot -DepotUrl C:\Datei-pfad\`*`Offline-Paket`*`.zip` aus.

   Das Cmdlet gibt mindestens ein `SoftwareDepot`-Objekt zurück.

2. Führen Sie das `Get-EsxImageProfile`-Cmdlet aus, um alle Image-Profile in allen derzeit sichtbaren Depots aufzulisten.

   Das cmdlet gibt alle verfügbaren Profile zurück. Sie können Ihre Suche mithilfe der optionalen Argumente zum Filtern der Ausgabe einschränken.

3. Klonen Sie das Profil.

   ```
   New-EsxImageProfile -CloneProfile My_Profile -Name "Test Profile 42" -Vendor "My Vendor"
   ```

   Von VMware und seinen Partnern veröffentlichte Image-Profile sind schreibgeschützt. Um Änderungen vorzunehmen, müssen Sie das Image-Profil klonen. Der Parameter `Anbieter` ist erforderlich.

4. Führen Sie das `Add-EsxSoftwarePackage`-Cmdlet aus, um ein neues Paket zu einem der Image-Profile hinzuzufügen.

   ```
   Add-EsxSoftwarePackage -ImageProfile My_Profile -SoftwarePackage partner-package
   ```

   Das cmdlet führt die Standard-Validierungstests für das Image-Profil durch. Ist die Validierung erfolgreich, gibt das cmdlet ein geändertes, validiertes Image-Profil zurück. Wenn das VIB, das Sie hinzufügen möchten, von einem anderen VIB abhängt, zeigt das cmdlet diese Informationen an, einschließlich des VIBs, das die Abhängigkeit beheben würde. Wenn die Akzeptanzebene des VIBs, das Sie hinzufügen möchten, niedriger als die Akzeptanzebene des Image-Profils ist, tritt ein Fehler auf.

Exportieren eines Image-Profils in ein ISO oder ein Offline-ZIP-Paket

Sie können ein Image-Profil in ein ISO-Image oder eine ZIP-Datei aus Komponenten-Dateien und -Ordnern exportieren. Sie können durch die einmalige Ausführung des cmdlets nicht beides erstellen. Sie können das ISO-Image als ESXi-Installationsprogramm verwenden oder für Upgrades das ISO in vSphere Update Manager hochladen. Sie können die ZIP-Datei, die Metadaten und die im Image-Profil angegebenen VIBs enthält, für Upgrades auf ESXi 5.0 und höher verwenden.

Voraussetzungen

Installieren Sie vSphere PowerCLI und alle erforderliche Software. Siehe „Installieren von vSphere ESXi Image Builder und erforderlicher Software“, auf Seite 159.

Vorgehensweise

1. Führen Sie in einer vSphere PowerCLI-Sitzung das Cmdlet `Add-EsxSoftwareDepot` für jedes Depot aus, mit dem Sie arbeiten möchten.

Option	Aktion
Remote-Depot	Führen Sie `Add-EsxSoftwareDepot -DepotUrl` *`URL_des_Depots`* aus.
ZIP-Datei	a Laden Sie die ZIP-Datei auf ein lokales Dateisystem herunter. b Führen Sie `Add-EsxSoftwareDepot -DepotUrl C:\Datei-pfad\`*`Offline-Paket`*`.zip` aus.

   Das Cmdlet gibt mindestens ein `SoftwareDepot`-Objekt zurück.

2 Führen Sie `Export-EsxImageProfile` aus, um das Image-Profil zu exportieren.

Format exportieren	Cmdlet
ISO-Images	`Export-EsxImageProfile` mit dem `-ExportToIso`-Parameter
Offline-Depot-ZIP-Dateien	`Export-EsxImageProfile` mit dem `-ExportToBundle`-Parameter

Beim ISO-Image validiert vSphere ESXi Image Builder die VIB-Signaturen, fügt dem Image die VIB-Binärdateien hinzu und lädt das Image an den angegebenen Speicherort herunter. Bei der ZIP-Datei validiert vSphere ESXi Image Builder die VIB-Signaturen und lädt die VIB-Binärdateien an den angegebenen Speicherort herunter.

Beispiel: Exportieren eines Image-Profils nach ISO

Beispiel: Exportieren eines Image-Profils in ein Offline-Paket

Führen Sie die folgenden Schritte aus, um ein Image-Profil in ein ISO-Image oder eine ZIP-Datei aus Komponentendateien und -ordnern zu exportieren.

1 Fügen Sie das Software-Depot hinzu.

```
Add-EsxSoftwareDepot -DepotUrl url_or_file
```

2 Zeigen Sie alle verfügbaren Image-Profile an, um den Namen des zu exportierenden Image-Profils zu suchen.

```
Get-EsxImageProfile
```

3 Exportieren Sie das Image-Profil.

```
Export-EsxImageProfile -ImageProfile "myprofile" -ExportToIso -FilePath iso_name
```

1 Fügen Sie das Software-Depot hinzu.

```
Add-EsxSoftwareDepot -DepotUrl url_or_file
```

2 Zeigen Sie alle verfügbaren Image-Profile an, um den Namen des zu exportierenden Image-Profils zu suchen.

```
Get-EsxImageProfile
```

3 Exportieren Sie das Image-Profil.

```
Export-EsxImageProfile -ImageProfile "myprofile" -ExportToBundle -FilePath C:\my_bundle.zip
```

Weiter

Verwenden Sie das ISO-Image in einer ESXi-Installation oder laden Sie es in Update Manager hoch, um Updates durchzuführen.

Verwenden Sie die ZIP-Datei für das Upgrade einer ESXi-Installation.

- Importieren Sie die ZIP-Datei zur Verwendung mit Patch-Baselines in vSphere Update Manager.
- Laden Sie die ZIP-Datei in einen ESXi-Host oder einen Datenspeicher herunter und führen Sie `esxcli software vib`-Befehle aus, um die VIBs in die ZIP-Datei zu importieren.

Informationen finden Sie in der Dokumentation *vSphere-Upgrade*.

Beibehalten von Image-Profilen über Sitzungen hinweg

Wenn Sie ein Image-Profil erstellen und die vSphere PowerCLI-Sitzung beenden, steht das Image-Profil nicht mehr zur Verfügung, wenn Sie eine neue Sitzung starten. Sie können das Image-Profil in ein ZIP-Datei-Software-Depot exportieren und dieses Depot in der nächsten Sitzung hinzufügen.

Voraussetzungen

Installieren Sie vSphere PowerCLI und alle erforderliche Software. Siehe „Installieren von vSphere ESXi Image Builder und erforderlicher Software“, auf Seite 159.

Vorgehensweise

1 Erstellen Sie in einer vSphere PowerCLI-Sitzung ein Image-Profil, indem Sie z. B. ein vorhandenes Image-Profil klonen und ein VIB hinzufügen.

2 Exportieren Sie das Image-Profil in eine ZIP-Datei, indem Sie `Export-EsxImageProfile` mit dem Parameter `ExportToBundle` aufrufen.

```
Export-EsxImageProfile    -ImageProfile "my_profile" -ExportToBundle -FilePath
                "C:\isos\temp-base-plus-vib25.zip"
```

3 Beenden Sie die vSphere PowerCLI-Sitzung.

4 Wenn Sie eine neue vSphere PowerCLI-Sitzung starten, fügen Sie das Depot hinzu, das Ihr Image-Profil enthält, um darauf zuzugreifen.

```
Add-EsxSoftwareDepot "C:\isos\temp-base-plus-vib25.zip"
```

Vergleichen von Image-Profilen

Mit dem `Compare-EsxImageProfile`-Cmdlet können Sie zwei Image-Profile vergleichen, um beispielsweise festzustellen, ob sie dieselbe VIB-Liste oder Akzeptanzebene aufweisen. Mithilfe der PowerShell-Vergleichsoperatoren können Sie Image-Profile oder deren Eigenschaften ebenfalls vergleichen.

Voraussetzungen

Installieren Sie vSphere PowerCLI und alle erforderliche Software. Siehe „Installieren von vSphere ESXi Image Builder und erforderlicher Software“, auf Seite 159.

Vorgehensweise

1 Führen Sie in einer vSphere PowerCLI-Sitzung das Cmdlet `Add-EsxSoftwareDepot` für jedes Depot aus, mit dem Sie arbeiten möchten.

Option	Aktion
Remote-Depot	Führen Sie `Add-EsxSoftwareDepot -DepotUrl` *`URL_des_Depots`* aus.
ZIP-Datei	a Laden Sie die ZIP-Datei auf ein lokales Dateisystem herunter. b Führen Sie `Add-EsxSoftwareDepot -DepotUrl C:\Dateipfad\`*`Offline-Paket`*`.zip` aus.

Das Cmdlet gibt mindestens ein `SoftwareDepot`-Objekt zurück.

2 (Optional) Führen Sie das `Get-EsxImageProfile`-Cmdlet aus, um alle Image-Profile in allen verfügbaren Depots aufzulisten.

In der Liste können Sie die Namen der Image-Profile suchen, die Sie vergleichen möchten.

3 Weisen Sie den Image-Profilen vor dem Vergleichen Variablen zu.

   Beispielsweise können Sie die Variablen `$imageProfile1` und `$imageProfile2` für die Namen der verglichenen Image-Profile erstellen.

```
$imageProfile1
                = Get-EsxImageProfile -Name "ImageProfile1"
$imageProfile2
                = Get-EsxImageProfile -Name "ImageProfile2"
```

4 Vergleichen Sie die beiden Image-Profile mit dem `Compare-EsxImageProfile`-Cmdlet oder dem Vergleichsoperator `-eq`, der einen booleschen Wert zurückgibt.

   - Vergleichen Sie die beiden Image-Profile mit dem `Compare-EsxImageProfile`-Cmdlet, um eine vollständige Beschreibung der Unterschiede zu erhalten.

```
Compare-EsxImageProfile -ReferenceProfile
                     $imageProfile1 -ComparisonProfile $imageProfile2
```

   - Vergleichen Sie die beiden Image-Profile anhand der VIB-Liste und der Akzeptanzebene mithilfe des Vergleichsoperators `-eq`.

```
if ($imageProfile1 -eq $imageProfile2) {
   Write-host "Successfully verified that both image profiles are equal."
} else {
   Write-host "Failed to verify that the image profiles are equal."
}
```

   - Vergleichen Sie die beiden Image-Profile anhand einer bestimmten Eigenschaft mithilfe des Vergleichsoperators `-eq`.

```
if ($imageProfile1.vendor -eq $imageProfile2.vendor) {
   Write-host "Successfully verified that both image profiles are equal."
} else {
   Write-host "Failed to verify that the image profiles are equal."
}
```

Vergleichen von VIBs

Mithilfe der PowerShell-Vergleichsoperatoren können Sie zwei VIBs oder deren Eigenschaften vergleichen.

Voraussetzungen

Installieren Sie vSphere PowerCLI und alle erforderliche Software. Siehe „Installieren von vSphere ESXi Image Builder und erforderlicher Software“, auf Seite 159.

Vorgehensweise

1 Führen Sie in einer vSphere PowerCLI-Sitzung das Cmdlet `Add-EsxSoftwareDepot` für jedes Depot aus, mit dem Sie arbeiten möchten.

Option	Aktion
Remote-Depot	Führen Sie `Add-EsxSoftwareDepot -DepotUrl` *`URL_des_Depots`* aus.
ZIP-Datei	a Laden Sie die ZIP-Datei auf ein lokales Dateisystem herunter. b Führen Sie `Add-EsxSoftwareDepot -DepotUrl C:\Datei-pfad\`*`Offline-Paket`*`.zip` aus.

   Das Cmdlet gibt mindestens ein `SoftwareDepot`-Objekt zurück.

2 (Optional) Führen Sie das `Get-EsxSoftwarePackage`-Cmdlet aus, um alle verfügbaren VIBs anzuzeigen.

   In der Liste können Sie die Namen der VIBs suchen, die Sie vergleichen möchten.

3 Weisen Sie den VIBs vor dem Vergleichen Variablen zu.

   Beispielsweise können Sie die Variablen `$vib1` und `$vib2` für die Namen der verglichenen VIBs erstellen.

```
$vib1 = Get-EsxSoftwarePackage -Name "ReferenceVIB"
$vib2 = Get-EsxSoftwarePackage -Name "ComparisonVIB"
```

4 Verwenden Sie einen Vergleichsoperator zum Vergleichen der VIBs anhand des Inhalts und der Akzeptanzebene oder anhand einer bestimmten Eigenschaft.

   - Vergleichen Sie die beiden VIBs anhand des Inhalts und der Akzeptanzebene.

```
if ($vib1 -eq $vib2) {
   Write-host "Successfully verified that both VIBs are equal."
} else {
   Write-host "Failed to verify that the VIBs are equal."
}
```

   - Vergleichen Sie eine bestimmte Eigenschaft der VIBs mithilfe eines Vergleichsoperators wie beispielsweise `-eq`, `-lt`, `-le`, `-gt` oder `-ge`.

```
if ($vib1.VersionObject -lt $vib2.VersionObject) {
   Write-host "Successfully verified that both the VIBs are equal."
} else {
   Write-host "Failed to verify that the VIBs are equal."
}
```

Arbeiten mit Akzeptanzebenen

Hosts, Image-Profile und einzelne VIBs verfügen über Akzeptanzebenen. VIB-Akzeptanzebenen zeigen, wie das VIB getestet wurde. Das Verständnis, was jede Akzeptanzebene bedeutet, wie die Ebenen geändert werden und welche Auswirkungen eine Änderung hat, ist ein wichtiger Bestandteil der Installation und der Update-Vorgänge.

Akzeptanzebenen werden für Hosts, Image-Profile und einzelne VIBs festgelegt. Die Standard-Akzeptanzebene für ein ESXi-Image oder ein Image-Profil ist „PartnerSupported“.

Hostakzeptanzebenen

Die Akzeptanzebene des Hosts bestimmt, welche VIBs Sie auf einem Host installieren können. Sie können mithilfe der ESXCLI-Befehle die Akzeptanzebene eines Hosts ändern. Standardmäßig haben ESXi-Hosts die Akzeptanzebene „PartnerSupported“, um auf einfache Art Updates mit PartnerSupported-VIBs zu ermöglichen.

Hinweis VMware unterstützt Hosts auf PartnerSupported-Akzeptanzebene. Bei Problemen mit einzelnen VIBs mit PartnerSupported-Akzeptanzebene wenden Sie sich an den Support des Partners.

Akzeptanzebenen des Image-Profils

Die Akzeptanzebene des Image-Profils wird auf die niedrigste im Image-Profil vorhandene VIB-Akzeptanzebene festgelegt. Wenn Sie ein VIB mit einer niedrigen Akzeptanzebene zu einem Image-Profil hinzufügen möchten, können Sie die Akzeptanzebene des Image-Profils mit dem `Set-EsxImageProfile`-cmdlet ändern. Siehe „Festlegen der Akzeptanzebene des Image-Profils“, auf Seite 168.

Der vSphere Update Manager zeigt die Akzeptanzebene selbst nicht an. Verwenden Sie vSphere ESXi Image Builder-Cmdlets, um die Informationen zur Akzeptanzebene für VIBs und Image-Profile abzurufen.

VIB-Akzeptanzebenen
Die Akzeptanzebene eines VIB wird beim Erstellen des VIB festgelegt. Nur der VIB-Ersteller kann die Akzeptanzebene festlegen.

Wenn Sie versuchen, einen Host mit einem Image-Profil oder VIB bereitzustellen, das über eine niedrigere Akzeptanzebene als der Host verfügt, tritt ein Fehler auf. Ändern Sie die Akzeptanzebene des Hosts, um das Image-Profil oder das VIB zu installieren. Siehe „Ändern der Hostakzeptanzebene", auf Seite 167. Durch das Ändern der Akzeptanzebene des Hosts wird das Support-Level für diesen Host geändert.

Die Akzeptanzebene eines Hosts, Image-Profils oder VIB ermöglicht Ihnen zu ermitteln, wer das VIB getestet hat und wer es unterstützt. VMware unterstützt die folgenden Akzeptanzebenen.

VMwareCertified
Die Akzeptanzebene „VMwareCertified" hat die strengsten Anforderungen. VIBs dieser Ebene unterliegen einer gründlichen Prüfung entsprechend den internen VMware-Qualitätssicherungstests für die gleiche Technologie. Heute werden nur IOVP-Treiber auf dieser Ebene veröffentlicht. VMware übernimmt Support-Anrufe für VIBs dieser Akzeptanzebene.

VMwareAccepted
VIBs dieser Akzeptanzebene unterliegen einer Verifizierungsprüfung; es wird jedoch nicht jede Funktion der Software in vollem Umfang getestet. Der Partner führt die Tests durch und VMware verifiziert das Ergebnis. Heute gehören CIM-Anbieter und PSA-Plug-Ins zu den VIBs, die auf dieser Ebene veröffentlicht werden. VMware leitet Support-Anrufe für VIBs dieser Akzeptanzebene an die Support-Organisation des Partners weiter.

PartnerSupported
VIBs mit der Akzeptanzebene „PartnerSupported" werden von einem Partner veröffentlicht, dem VMware vertraut. Der Partner führt alle Tests durch. VMware überprüft die Ergebnisse nicht. Diese Ebene wird für eine neue oder nicht etablierte Technologie verwendet, die Partner für VMware-Systeme aktivieren möchten. Auf dieser Ebene sind heute Treiber-VIB-Technologien mit nicht standardisierten Hardwaretreibern, wie z. B. Infiniband, ATAoE und SSD. VMware leitet Support-Anrufe für VIBs dieser Akzeptanzebene an die Support-Organisation des Partners weiter.

CommunitySupported
Die Akzeptanzebene „CommunitySupported" ist für VIBs gedacht, die von Einzelpersonen oder Unternehmen außerhalb der VMware Partner-Programme erstellt wurden. VIBs auf dieser Ebene wurden nicht im Rahmen eines von VMware zugelassenen Testprogramms getestet und werden weder von VMware Technical Support noch von einem VMware-Partner unterstützt.

Ändern der Hostakzeptanzebene

Sie können die Host-Akzeptanzebene verringern, sodass sie mit der Akzeptanzebene für ein VIB oder Image-Profil, das Sie installieren möchten, übereinstimmt.

Die Akzeptanzebene jedes VIB auf einem Host muss mindestens so hoch wie die Akzeptanzebene des Hosts sein. Es ist beispielsweise nicht möglich, ein VIB mit der Akzeptanzebene „PartnerSupported" auf einem Host mit der Akzeptanzebene „VMwareAccepted" zu installieren. Sie müssen zunächst die Akzeptanzebene des Hosts verringern. Weitere Informationen zu Akzeptanzebenen finden Sie unter „Akzeptanzebenen", auf Seite 154.

Die Änderung der Hostakzeptanzebene zu CommunitySupported wirkt sich auf die Supportfähigkeit des Hosts aus und kann dessen Sicherheit beeinträchtigen.

Voraussetzungen

Installieren Sie vCLI oder stellen Sie die virtuelle vSphere Management Assistant (vMA)-Maschine bereit. Weitere Informationen hierzu finden Sie unter *Erste Schritte mit vSphere-Befehlszeilenschnittstellen*. Zur Fehlerbehebung führen Sie `esxcli`-Befehle in der ESXi Shell aus.

Vorgehensweise

1 Rufen Sie die Akzeptanzebene für das VIB oder das Image-Profil ab.

Option	Beschreibung
Informationen für alle VIBs anzeigen	`esxcli --server=server_name software sources vib list --depot=depot_URL`
Informationen für ein bestimmtes VIB anzeigen	`esxcli --server=server_name software sources vib list --viburl=vib_URL`
Informationen für alle Image-Profile anzeigen	`esxcli --server=server_name software sources profile list --depot=depot_URL`
Informationen für ein bestimmtes Image-Profil anzeigen	`esxcli --server=server_name software sources profile get --depot=depot_URL --profile=profile_name`

2 Die Hostakzeptanzebene anzeigen

```
esxcli --server=server_name software acceptance get
```

3 Die Akzeptanzebene des Hosts ändern

```
esxcli
        --server=server_name software acceptance set --level=acceptance_level
```

Der Wert für *acceptance_level* kann `VMwareCertified`, `VMwareAccepted`, `PartnerSupported` oder `CommunitySupported` sein. Bei den Werten für die *Akzeptanzebene* wird zwischen der Klein- und Großschreibung unterschieden.

HINWEIS Wenn der Host eine höhere Akzeptanzebene hat als das VIB oder das Image-Profil, das Sie hinzufügen möchten, können Sie Befehle im Namespace `esxcli software vib` oder `esxcli software profile` mit der Option `--force` ausführen. Wenn Sie die Option `--force` verwenden, wird eine Warnung angezeigt, weil Sie ein VIB oder Image-Profil mit einer niedrigeren Akzeptanzebene als der Akzeptanzebene des Hosts durchsetzen und Ihre Einrichtung nicht mehr konsistent ist. Die Warnung wird wiederholt, wenn Sie VIBs installieren, VIBs entfernen oder bestimmte andere Vorgänge auf dem Host durchführen, der inkonsistente Akzeptanzebenen hat.

Festlegen der Akzeptanzebene des Image-Profils

Wenn Sie einem Image-Profil ein VIB hinzufügen möchten und die VIB-Akzeptanzebene niedriger als die Akzeptanzebene des Image-Profils ist, können Sie das Image-Profil mit einer niedrigeren Akzeptanzebene klonen oder die Akzeptanzebene des Image-Profils ändern.

Als Akzeptanzebene eines Image-Profils können Sie VMwareCertified, VMwareAccepted, PartnerSupported oder CommunitySupported angeben. Wenn Sie die Akzeptanzebene verringern, ändert sich damit auch die Ebene der Unterstützung für das Image-Profil und die Hosts, die Sie damit bereitstellen. Weitere Informationen finden Sie unter „Akzeptanzebenen“, auf Seite 154.

Voraussetzungen

Installieren Sie vSphere PowerCLI und alle erforderliche Software. Siehe „Installieren von vSphere ESXi Image Builder und erforderlicher Software“, auf Seite 159.

Vorgehensweise

1 Führen Sie in einer vSphere PowerCLI-Sitzung das Cmdlet `Add-EsxSoftwareDepot` für jedes Depot aus, mit dem Sie arbeiten möchten.

Option	Aktion
Remote-Depot	Führen Sie `Add-EsxSoftwareDepot -DepotUrl` *`URL_des_Depots`* aus.
ZIP-Datei	a Laden Sie die ZIP-Datei auf ein lokales Dateisystem herunter. b Führen Sie `Add-EsxSoftwareDepot -DepotUrl C:\Datei-pfad\`*`Offline-Paket`*`.zip` aus.

Das Cmdlet gibt mindestens ein `SoftwareDepot`-Objekt zurück.

2 Rufen Sie die Akzeptanzebene für das Image-Profil ab.

```
Get-EsxImageProfile -Name string
```

3 Legen Sie die Akzeptanzebene des Image-Profils fest.

```
Set-EsxImageProfile -Name string -AcceptanceLevel level
```

vSphere ESXi Image Builder-Workflows

vSphere ESXi Image Builder-Workflows sind Beispiele der Verwendung von Cmdlets. Workflows stellen keine tatsächlichen Aufgaben dar, sondern sie veranschaulichen, wie Sie unterschiedliche Verwendungsarten eines cmdlets ausprobieren können. Administratoren, die die Workflows ausprobieren, profitieren von Erfahrungen mit vSphere PowerCLI, Microsoft PowerShell oder beidem.

Untersuchen von Depot-Inhalten

Sie können Software-Depots und VIBs mithilfe von vSphere ESXi Image Builder-Cmdlets untersuchen. Dabei können Sie Platzhalterzeichen verwenden. Alle Platzhalterausdrücke werden unterstützt.

Der Workflow selbst übergibt Parameter nach Namen. Mit Variablen können Sie Parameter jedoch auch als Objekte übergeben.

Zum Durchsuchen der Depot-Inhalte können Sie Filteroptionen und Platzhalterausdrücke verwenden.

Voraussetzungen

Stellen Sie sicher, dass vSphere PowerCLI und alle erforderlichen Softwareprodukte installiert sind. Siehe „Installieren von vSphere ESXi Image Builder und erforderlicher Software“, auf Seite 159.

Vorgehensweise

1 Führen Sie in einer vSphere PowerCLI-Sitzung das Cmdlet `Add-EsxSoftwareDepot` für jedes Depot aus, mit dem Sie arbeiten möchten.

Option	Aktion
Remote-Depot	Führen Sie `Add-EsxSoftwareDepot -DepotUrl` *`URL_des_Depots`* aus.
ZIP-Datei	a Laden Sie die ZIP-Datei auf ein lokales Dateisystem herunter. b Führen Sie `Add-EsxSoftwareDepot -DepotUrl C:\Datei-pfad\`*`Offline-Paket`*`.zip` aus.

Das Cmdlet gibt mindestens ein `SoftwareDepot`-Objekt zurück.

2 Rufen Sie Image-Profile ab.

   Sie können nach Anbieter, Namen und Akzeptanzebene filtern.

   - `Get-EsxImageProfiles`

     Gibt ein Array von `ImageProfile`-Objekten aus allen Depots zurück, die Sie zur Sitzung hinzugefügt haben.

   - `Get-EsxImageProfile -Vendor "C*"`

     Gibt alle Image-Profile zurück, die von einem Anbieter erstellt wurden, dessen Name mit dem Buchstaben C beginnt.

3 Rufen Sie Softwarepakete mit dem Cmdlet `Get-EsxSoftwarePackage` ab.

   Sie können beispielsweise nach Anbieter oder Version filtern und die standardmäßigen PowerShell-Platzhalterzeichen verwenden.

   - `Get-EsxSoftwarePackage -Vendor "V*"`

     Gibt alle Softwarepakete eines Anbieters zurück, dessen Name mit dem Buchstaben V beginnt.

   - `Get-EsxSoftwarePackage -Vendor "V*" -Name "*scsi*"`

     Gibt alle Softwarepakete mit `scsi` im Paketnamen von einem Anbieter zurück, dessen Name mit dem Buchstaben V beginnt.

   - `Get-EsxSoftwarePackage -Version "2.0*"`

     Gibt alle Softwarepakete zurück, deren Versionsname mit 2.0 beginnt.

4 Mit `-Newest` finden Sie das neueste Paket.

   - `Get-EsxSoftwarePackage -Vendor "V*" -Newest`

     Gibt das neueste Paket der Anbieter zurück, deren Name mit V beginnt, und zeigt die Informationen als Tabelle an.

   - `Get-EsxSoftwarePackage -Vendor "V*" -Newest | format-list`

     Gibt ausführliche Informationen zu jedem Softwarepaket über eine Pipeline zurück, welche die Ausgabe der Softwarepaketanforderung mit dem PowerShell-Cmdlet `format-list` verbindet.

5 Zeigen Sie die Liste der VIBs im Image-Profil an.

   ```
   (Get-EsxImageProfile -Name "Robin's Profile").VibList
   ```

   `VibList` ist eine Eigenschaft des `ImageProfile`-Objekts.

6 Sie können Softwarepakete, die vor oder nach einem bestimmten Datum veröffentlicht wurden, mithilfe des Parameters `CreatedBefore` oder `CreatedAfter` abrufen.

   ```
   Get-EsxSoftwarePackage -CreatedAfter 7/1/2010
   ```

Beispiel: Untersuchung von Depot-Inhalten mithilfe von Variablen

In diesem Workflowbeispiel werden Depot-Inhalte untersucht, indem Parameter als Objekte anstatt nach Namen übergeben werden. Dies erfolgt durch eine Variable, mit der auf die Position der Objekte zugegriffen wird. Sie können die folgenden Befehle der Reihe nach über die vSphere PowerCLI-Eingabeaufforderung ausführen. Ersetzen Sie Namen durch Namen, die für Ihre Installation geeignet sind.

```
Get-EsxSoftwarePackage -Vendor "V*"
Get-EsxSoftwarePackage -Vendor "V*" -Name "r*"
Get-EsxSoftwarePackage -Version "2.0*"
$ip1 = Get-EsxImageProfile -name ESX-5.0.0-123456-full
$ip1.VibList
Get-EsxSoftwarePackage -CreatedAfter 7/1/2010
```

Workflow für die Erstellung von Image-Profilen durch Klonen

Mit den Cmdlets in vSphere ESXi Image Builder können Sie prüfen, welche Depots verfügbar sind, einem Depot Inhalt hinzufügen, Informationen zu Image-Profilen einsehen und durch Klonen bestehender Image-Profile neue Image-Profile erstellen.

Veröffentlichte Profile sind in der Regel schreibgeschützt und können nicht geändert werden. Auch bei nicht schreibgeschützten veröffentlichten Profilen empfiehlt es sich jedoch, das Profil zu klonen, anstatt es zu ändern, da das ursprüngliche Profil durch die Änderungen verloren gehen würde. Sie können das ursprüngliche, unveränderte Profil nur wiederherstellen, indem Sie erneut eine Verbindung zu einem Depot herstellen.

Ein Workflow für das Klonen von Profilen kann das Überprüfen des aktuellen Systemstatus, das Hinzufügen eines Software-Depots und das Klonen des Profils umfassen.

Voraussetzungen

Stellen Sie sicher, dass vSphere PowerCLI und alle erforderlichen Softwareprodukte installiert sind. Siehe „Installieren von vSphere ESXi Image Builder und erforderlicher Software", auf Seite 159.

Vorgehensweise

1 Prüfen Sie in einem PowerShell-Fenster, ob für die aktuelle Sitzung Software-Depots definiert sind.

```
$DefaultSoftwareDepots
```

PowerShell gibt die aktuell definierten Depots zurück bzw. nichts, wenn Sie PowerShell gerade gestartet haben.

2 Wenn ein Depot, in dem das zu klonende Profil enthalten ist, in den Ergebnissen nicht erscheint, fügen Sie es der aktuellen Sitzung hinzu.

Option	Aktion
Remote-Depot	Führen Sie `Add-EsxSoftwareDepot -DepotUrl` *URL_des_Depots* aus.
ZIP-Datei	a Laden Sie die ZIP-Datei auf einen lokalen Dateipfad herunter. b Führen Sie `Add-EsxSoftwareDepot -DepotUrl C:\Datei-pfad\`*Offline-Paket*`.zip` aus.

PowerShell fügt das angegebene Depot zu Ihrer aktuellen Sitzung hinzu und listet alle aktuellen Depots auf.

3 (Optional) Klicken Sie auf die Variable `$DefaultSoftwareDepots`, die nun das neu hinzugefügte Depot zurückgibt.

4 Zeigen Sie alle verfügbaren Image-Profile an.

```
Get-EsxImageProfile
```

5 Um ein Image-Profil zu klonen, geben Sie dessen Namen, einen neuen Namen für das neue Profil und einen Namen für den Hersteller ein.

```
$ip = New-EsxImageProfile -CloneProfile base-tbd-v1 -Name "Test Profile 42" -Vendor "Ven-
dor20"
```

6 (Optional) Sie sehen das neue erstellte Profil (`$ip`).

PowerShell gibt die Informationen zum Image-Profil im tabellarischen Format zurück.

```
Name              Vendor       Last Modified        Acceptance Level
----              ------       -------------        ----------------
Test Profile 42   Vendor20     9/15/2010 5:45:43... PartnerSupported
```

Beispiel: Erstellen eines Image-Profils durch Klonen mithilfe von Variablen

Dieses Workflowbeispiel wiederholt die Schritte des Workflows, indem Parameter als Objekte anstatt nach Namen übergeben werden. Dies erfolgt durch eine Variable, mit der auf die Position der Objekte zugegriffen wird. Sie können die folgenden Cmdlets der Reihe nach über die vSphere PowerCLI-Eingabeaufforderung ausführen.

```
$DefaultSoftwareDepots
Add-EsxSoftwareDepot -DepotUrl depot_url
$DefaultSoftwareDepots
$profs = Get-EsxImageProfile
$profs
$ip = New-EsxImageProfile -CloneProfile $profs[2] -Name "new_profile_name" -Vendor "my_vendor"
$ip
```

Workflow für das Erstellen neuer Image-Profile

In den meisten Situationen erstellen Sie ein Image-Profil, indem Sie ein vorhandenes Profil klonen. Einige VMware-Kunden oder -Partner müssen möglicherweise ein Image-Profil neu erstellen. Achten Sie sorgfältig auf Abhängigkeiten und Akzeptanzebenen, wenn Sie ein Image-Profil von Grund auf neu erstellen.

Das System erwartet, dass die Akzeptanzebene der VIBs, die Sie zum Basis-Image hinzufügen, mindestens so hoch ist wie die Ebene des Basis-Images. Wenn Sie ein VIB mit einer niedrigeren Akzeptanzebene zu einem Image-Profil hinzufügen müssen, müssen Sie die Akzeptanzebene des Image-Profils verringern. Weitere Informationen finden Sie unter „Festlegen der Akzeptanzebene des Image-Profils“, auf Seite 168.

Als Alternative zum Angeben der Parameter in der Befehlszeile können Sie den PowerShell-Aufforderungsmechanismus verwenden, um String-Parameter anzugeben. Der Aufforderungsmechanismus funktioniert nicht bei anderen Parametern, wie z. B. Objekten.

Voraussetzungen

- vSphere PowerCLI und die erforderliche Software sind installiert. Siehe „Installieren von vSphere ESXi Image Builder und erforderlicher Software“, auf Seite 159.
- Sie haben Zugriff auf ein Depot, das ein Basis-Image und ein oder mehrere VIBs enthält. VMware und VMware-Partner verfügen über öffentliche Depots, auf die über eine URL zugegriffen werden kann. VMware oder VMware-Partner können eine ZIP-Datei erstellen, die Sie in Ihre lokale Umgebung extrahieren und auf die Sie über einen Dateipfad zugreifen können.

Vorgehensweise

1. Führen Sie in einer vSphere PowerCLI-Sitzung das Cmdlet `Add-EsxSoftwareDepot` für jedes Depot aus, mit dem Sie arbeiten möchten.

Option	Aktion
Remote-Depot	Führen Sie `Add-EsxSoftwareDepot -DepotUrl` *`URL_des_Depots`* aus.
ZIP-Datei	a Laden Sie die ZIP-Datei auf ein lokales Dateisystem herunter. b Führen Sie `Add-EsxSoftwareDepot -DepotUrl C:\Dateipfad\`*`Offline-Paket`*`.zip` aus.

   Das Cmdlet gibt mindestens ein `SoftwareDepot`-Objekt zurück.

2. Führen Sie das `Get-EsxImageProfile`-Cmdlet aus, um alle Image-Profile in allen derzeit sichtbaren Depots aufzulisten. Sie können Ihre Suche mithilfe der optionalen Argumente zum Filtern der Ausgabe einschränken.

   ```
   Get-EsxSoftwarePackage -CreatedAfter 7/1/2010
   ```

3 Erstellen Sie ein neues Profil, weisen Sie ihm einen Namen und einen Anbieter zu und fügen Sie ein Basispaket hinzu.

```
New-EsxImageProfile -NewProfile -Name "Test #2" -vendor "Vendor42" -SoftwarePackage esx-ba-
se[0],esx-xlibs[0]
```

Das Beispiel verwendet das Paket „esx-base". In den meisten Fällen fügen Sie das Paket „esx-base" hinzu, wenn Sie ein Image-Profil neu erstellen. Namen, die Leerzeichen enthalten, werden in Anführungszeichen gesetzt.

4 Verwenden Sie eine Pipelline, um das neue Image-Profil an `format-list` zu übergeben und detaillierte Informationen zum neuen Paket zu erhalten.

```
(Get-EsxImageProfile -Name "Test #2").VibList | format-list
```

Beispiel: Erstellen von Image-Profilen von Grund auf mithilfe von Variablen

Dieser Befehl wiederholt die Schritte des Workflows, übergibt jedoch Parameter als Objekte, auf die nach der Position in einer Variablen zugegriffen wird, anstatt Parameter nach Name zu übergeben. Sie können die folgenden Befehle der Reihe nach über die vSphere PowerCLI-Eingabeaufforderung ausführen.

```
Add-EsxSoftwareDepot depoturl
$pkgs = Get-EsxSoftwarePackage -CreatedAfter 7/1/2010
$ip2 = New-EsxImageProfile -NewProfile -Name "Test #2" -vendor "Vendor42" -SoftwarePackage
$pkgs[0]
$ip2.VibList | format-list
```

Workflow zum Bearbeiten von Image-Profilen

Sie können ein benutzerdefiniertes Image erstellen, indem Sie ein Image-Profil klonen und bearbeiten. Sie können im vorhandenen Profil ein oder mehrere VIBs hinzufügen oder ersetzen. Wenn das Hinzufügen oder Ersetzen von VIBs zur Folge haben könnte, dass das Image-Profil nicht ordnungsgemäß arbeitet, tritt ein Fehler auf.

Voraussetzungen

- vSphere PowerCLI und die erforderliche Software sind installiert. Siehe „Installieren von vSphere ESXi Image Builder und erforderlicher Software", auf Seite 159.
- Sie haben Zugriff auf ein Depot, das ein Basis-Image und ein oder mehrere VIBs enthält. VMware und VMware-Partner stellen öffentliche Depots zur Verfügung, auf die über eine URL zugegriffen werden kann. VMware oder VMware-Partner können eine ZIP-Datei erstellen, die Sie in Ihre lokale Umgebung herunterladen und auf die Sie über einen Dateipfad zugreifen können.

Vorgehensweise

1 Führen Sie in einer vSphere PowerCLI-Sitzung das Cmdlet `Add-EsxSoftwareDepot` für jedes Depot aus, mit dem Sie arbeiten möchten.

Option	Aktion
Remote-Depot	Führen Sie `Add-EsxSoftwareDepot -DepotUrl` *`URL_des_Depots`* aus.
ZIP-Datei	a Laden Sie die ZIP-Datei auf ein lokales Dateisystem herunter. b Führen Sie `Add-EsxSoftwareDepot -DepotUrl C:\Datei-pfad\`*`Offline-Paket`*`.zip` aus.

Das Cmdlet gibt mindestens ein `SoftwareDepot`-Objekt zurück.

2 Übergeben Sie das Image-Profil, das Sie bearbeiten möchten, per Pipeline an `format-list`, um ausführliche Informationen anzuzeigen.

In diesem Beispiel enthält das Image-Profil, das unter „Workflow für das Erstellen neuer Image-Profile“, auf Seite 172 erstellt wurde, nur das Basis-Image. Ein neu erstelltes Image-Profil ist nicht im Depot enthalten. Stattdessen greifen Sie über den Namen auf das Image-Profil zu, oder indem Sie es an eine Variable binden.

```
Get-EsxImageProfile "Test #2" | format-list
```

PowerShell gibt die Informationen zurück.

```
Name            : Test #2
Anbieter           : Vendor42
...
VibList          : {esx-base 5.0.0.-...,}
```

3 (Optional) Wenn Sie ein VIB mit einer niedrigeren Akzeptanzebene als der Ebene des Image-Profils hinzufügen, ändern Sie die Akzeptanzebene des Image-Profils.

```
Set-EsxImageProfile -ImageProfile "Test #2" -AcceptanceLevel VMwareAccepted
```

PowerShell gibt die Informationen zum geänderten Profil im tabellarischen Format zurück.

```
Name           Vendor           Last Modified       Acceptance Level
----           ------           -------------       ----------------
Test #2        Vendor42         9/22/2010 12:05:... VMwareAccepted
```

4 Fügen Sie ein Softwarepaket (VIB) zum Image-Profil hinzu. Sie können das Paket nach Namen hinzufügen.

```
Add-EsxSoftwarePackage -ImageProfile "Test #2"
                -SoftwarePackage NewPack3
```

PowerShell gibt die Informationen zum Image-Profil im tabellarischen Format zurück.

```
Name           Vendor           Last Modified       Acceptance Level
----           ------           -------------       ----------------
Test #2        Vendor42         9/22/2010 12:05:... VMwareAccepted
```

Hinweis Wenn beim Hinzufügen des Softwarepakets ein Fehler auftritt, kann dies an einem Problem mit Akzeptanzebenen liegen; siehe „Arbeiten mit Akzeptanzebenen“, auf Seite 166.

5 Zeigen Sie erneut das Image-Profil an.

```
Get-EsxImageProfile "Test #2" | format-list
```

Die VIB-Liste wird aktualisiert, sodass sie das neue Softwarepaket enthält, und die Informationen werden angezeigt.

```
Name            : Test #2
Anbieter           : Vendor42
...
VibList          : {esx-base 5.0.0.-..., NewPack3}
```

Beispiel: Bearbeiten von Image-Profilen mithilfe von Variablen

Diese cmdlet-Sequenz wiederholt die Schritte des Workflows, übergibt jedoch Parameter als Objekte, auf die nach der Position in einer Variablen zugegriffen wird, anstatt Parameter nach Name zu übergeben. Sie können die folgenden cmdlets der Reihe nach über die vSphere PowerCLI-Eingabeaufforderung ausführen.

```
Add-EsxSoftwareDepot -DepotUrl depot_url
$ip2 = Get-EsxImageProfile -name "Test #2"
$ip2 | format-list
Set-EsxImageProfile -ImageProfile $ip2 -AcceptanceLevel VMwareAccepted
Add-EsxImageSoftwarePackage -ImageProfile $ip2 -SoftwarePackage NewPack3
$ip2 | format-list
```

Einrichten von ESXi 5

Diese Themen befassen sich mit der Verwendung der Benutzerschnittstelle der direkten Konsole und dem Konfigurieren von Standardwerten für ESXi.

Dieses Kapitel behandelt die folgenden Themen:

Autokonfiguration von ESXi

Wenn Sie den ESXi-Host zum ersten Mal oder nach dem Zurücksetzen der Konfigurationsstandardeinstellungen einschalten, wird der Host in eine Autokonfigurationsphase versetzt. In dieser Phase werden die Systemnetzwerk- und Speichergeräte mit Standardwerten konfiguriert.

Standardmäßig konfiguriert DHCP (Dynamic Host Configuration Protocol) die IP-Einstellungen. Alle sichtbaren internen leeren Festplatten werden mit VMFS (virtual machine file system) formatiert, damit virtuelle Maschinen darauf gespeichert werden können.

Grundlegendes zur Direct Console ESXi Interface (ESXi-Schnittstelle der direkten Konsole)

Sie können die Schnittstelle der direkten Konsole zum anfänglichen Konfigurieren und zur anfänglichen Fehlebehebung von ESXi verwenden.

Schließen Sie eine Tastatur und einen Bildschirm am Host an, um die direkte Konsole zu verwenden. Nachdem der Host die Autokonfigurationsphase abgeschlossen hat, erscheint die direkte Konsole auf dem Bildschirm. Sie können die Standard-Netzwerkkonfiguration anzeigen und alle Einstellungen ändern, die nicht mit Ihrer Netzwerkumgebung kompatibel sind.

Über die direkte Konsole können Sie die folgenden wichtigen Aufgaben ausführen:

- Konfigurieren von Hosts
- Den Administratorzugriff einrichten
- Fehlerbehebung

Sie können auch vSphere Web Client verwenden, um den Host mithilfe von vCenter Server zu verwalten.

Tabelle 5-1. Navigieren in der direkten Konsole

Aktion	Schlüssel
Anzeigen und Ändern der Konfiguration	F2
Ändern Sie Ihre Oberfläche in einen Modus mit einem hohen Kontrast	F4
Herunterfahren und Neustarten des Hosts	F12
Anzeigen des VMkernel-Protokolls	Alt+F12
Wechseln zur Shell-Konsole	Alt+F1
Wechseln zur Benutzerschnittstelle der direkten Konsole	Alt+F2
Verschieben der Auswahl zwischen Feldern	Pfeiltasten
Auswählen eines Menüpunkts	Eingabetaste
Umschalten eines Wertes	Leertaste
Bestätigen weitreichender Befehle, z. B. Zurücksetzen auf die Konfigurationsstandardeinstellungen	F11
Speichern und beenden	Eingabetaste
Beenden ohne Speichern	Esc
Beenden von Systemprotokollen	q

Konfigurieren der Tastaturbelegung für die direkte Konsole

Sie können die Belegung der Tastatur konfigurieren, mit der Sie die direkte Konsole bedienen.

Vorgehensweise

1. Wählen Sie in der direkten Konsole **Tastatur konfigurieren**, und drücken Sie die Eingabetaste.
2. Wählen Sie die zu verwendende Belegung aus.
3. Drücken Sie die Leertaste, um Optionen zu aktivieren oder zu deaktivieren.
4. Drücken Sie die Eingabetaste.

Erstellen eines Sicherheitsbanners für die direkte Konsole

Ein Sicherheitsbanner ist eine Meldung, die auf dem Begrüßungsbildschirm der direkten Konsole angezeigt wird.

Vorgehensweise

1. Stellen Sie vom vSphere Web Client aus eine Verbindung zu vCenter Server her.
2. Wählen Sie den Host in der Bestandsliste aus.
3. Klicken Sie auf die Registerkarte **Verwalten**.
4. Klicken Sie auf **Einstellungen**.
5. Klicken Sie unter „System“ auf **Erweiterte Systemeinstellungen**.
6. Wählen Sie **Anmerkungen**.
7. Klicken Sie auf das Symbol „Bearbeiten“.
8. Geben Sie eine Sicherheitsmeldung ein.

Die Meldung wird auf dem Begrüßungsbildschirm der direkten Konsole angezeigt.

Umleiten der direkten Konsole auf eine serielle Schnittstelle

Zur Remoteverwaltung Ihres ESXi-Host von einer seriellen Konsole aus können Sie die direkte Konsole auf einen seriellen Port umleiten.

vSphere unterstützt den VT100-Terminaltyp und den PuTTy-Terminalemulator zur Anzeige der direkten Konsole über den seriellen Port.

Sie haben verschiedene Möglichkeiten, die direkte Konsole auf einen seriellen Port umzuleiten.

- Umleiten der direkten Konsole auf einen seriellen Port durch manuelles Einstellen der Startoptionen auf Seite 180

  Wenn Sie die direkte Konsole auf einen seriellen Port umleiten, indem Sie die Startoptionen festlegen, bleibt die Änderung für nachfolgende Startvorgänge nicht erhalten.

- Umleiten der direkten Konsole auf einen seriellen Port vom vSphere Web Client aus auf Seite 180

  Sie können den ESXi-Host remote von einer Konsole aus verwalten, die mit dem seriellen Port verbunden ist, indem Sie die direkte Konsole zu einem der beiden seriellen Ports com1 und com2 umleiten. Wenn Sie den vSphere Web Client verwenden, um die direkte Konsole auf einen seriellen Port umzuleiten, wird die eingestellte Startoption bei nachfolgenden Startvorgängen beibehalten.

- Umleiten der direkten Konsole auf einen seriellen Port in einem Host, der mit Auto Deploy bereitgestellt wurde auf Seite 181

  Nachdem Sie die direkte Konsole auf einen seriellen Port umgeleitet haben, können Sie diese Einstellung in das Hostprofil übernehmen, das beibehalten wird, wenn Sie den Host mit Auto Deploy erneut bereitstellen.

Umleiten der direkten Konsole auf einen seriellen Port durch manuelles Einstellen der Startoptionen

Wenn Sie die direkte Konsole auf einen seriellen Port umleiten, indem Sie die Startoptionen festlegen, bleibt die Änderung für nachfolgende Startvorgänge nicht erhalten.

Voraussetzungen

Stellen Sie sicher, dass der serielle Port nicht für die serielle Protokollierung und serielles Debuggen verwendet wird.

Vorgehensweise

1 Starten Sie den Host.

2 Wenn das Fenster zum Laden des VMware Hypervisors erscheint, drücken Sie Umschalt+O, um die Startoptionen zu bearbeiten.

3 Deaktivieren Sie logPort und gdbPort auf COM1 und stellen Sie tty2Port auf COM1 ein, indem Sie die folgenden Startoptionen eingeben:

```
"gdbPort=none logPort=none tty2Port=com1";
```

  Wenn Sie stattdessen COM2 verwenden möchten, ersetzen Sie `com1` durch `com2`.

Die direkte Konsole wird auf den seriellen Port umgeleitet, bis Sie den Host neu starten. Um die direkte Konsole für nachfolgende Startvorgänge umzuleiten, lesen Sie „Umleiten der direkten Konsole auf einen seriellen Port vom vSphere Web Client aus“, auf Seite 180

Umleiten der direkten Konsole auf einen seriellen Port vom vSphere Web Client aus

Sie können den ESXi-Host remote von einer Konsole aus verwalten, die mit dem seriellen Port verbunden ist, indem Sie die direkte Konsole zu einem der beiden seriellen Ports com1 und com2 umleiten. Wenn Sie den vSphere Web Client verwenden, um die direkte Konsole auf einen seriellen Port umzuleiten, wird die eingestellte Startoption bei nachfolgenden Startvorgängen beibehalten.

Voraussetzungen

- Stellen Sie sicher, dass Sie vom vSphere Web Client aus auf den Host zugreifen können.
- Stellen Sie sicher, dass der serielle Port nicht für die serielle Protokollierung und das serielle Debuggen oder die ESX Shell (tty1Port) verwendet wird.

Vorgehensweise

1 Stellen Sie vom vSphere Web Client aus eine Verbindung zu vCenter Server her.

2 Wählen Sie den Host in der Bestandsliste aus.

3 Klicken Sie auf die Registerkarte **Verwalten**.

4 Klicken Sie auf **Einstellungen**.

5 Klicken Sie unter „System“ auf **Erweiterte Systemeinstellungen**.

6 Stellen Sie sicher, das die Felder **VMkernel.Boot.logPort** und **VMkernel.Boot.gdbPort** nicht für die Verwendung des COM-Ports eingestellt sind, an die Sie die direkte Konsole umleiten möchten.

7 Legen Sie **VMkernel.Boot.tty2Port** auf den seriellen Port fest, an die Sie die direkte Konsole umleiten möchten: `com1` oder `com2`.

8 Starten Sie den Host neu.

Sie können nun den ESXi-Host remote von einer Konsole aus verwalten, die an den seriellen Port angeschlossen ist.

Umleiten der direkten Konsole auf einen seriellen Port in einem Host, der mit Auto Deploy bereitgestellt wurde

Nachdem Sie die direkte Konsole auf einen seriellen Port umgeleitet haben, können Sie diese Einstellung in das Hostprofil übernehmen, das beibehalten wird, wenn Sie den Host mit Auto Deploy erneut bereitstellen.

Voraussetzungen

Der serielle Port darf nicht bereits für die serielle Protokollierung und das serielle Debuggen verwendet werden.

Vorgehensweise

1 Stellen Sie vom vSphere Web Client aus eine Verbindung zu vCenter Server her.

2 Wählen Sie den Host in der Bestandsliste aus.

3 Klicken Sie auf die Registerkarte **Verwalten**.

4 Wählen Sie **Einstellungen**.

5 Wählen Sie **Erweiterte Systemeinstellungen**.

6 Stellen Sie sicher, das die Felder **VMkernel.Boot.logPort** und **VMkernel.Boot.gdbPort** nicht für die Verwendung des COM-Ports eingestellt sind, an die Sie die direkte Konsole umleiten möchten.

7 Legen Sie **VMkernel.Boot.tty2Port** auf den seriellen Port fest, an die Sie die direkte Konsole umleiten möchten: `com1` oder `com2`.

8 Klicken Sie auf **OK**.

9 Speichern Sie das Hostprofil und hängen Sie den Host an das Profil an. Informationen finden Sie in der Dokumentation *vSphere-Hostprofile*.

Die Einstellung zur Umleitung der direkten Konsole auf einen seriellen Port wird von vCenter Server gespeichert und beibehält, wenn Sie den Host mit Auto Deploy erneut bereitstellen.

Festlegen des Kennworts für das Administratorkonto

Sie können die direkte Konsole verwenden, um das Kennwort für das Administratorkonto (Root) festzulegen.

Der administrative Benutzername für den ESXi-Host lautet „root“. Standardmäßig ist der Administratorkennwort nicht gesetzt.

Vorgehensweise

1 Wählen Sie an der direkten Konsole die Option **Kennwort konfigurieren** aus.

2 (Optional) Wenn bereits ein Kennwort eingerichtet wurde, geben Sie es unter **Altes Kennwort** ein und drücken Sie die Eingabetaste.

3 Geben Sie unter **Neues Kennwort** ein neues Kennwort ein und drücken Sie die Eingabetaste.

4 Geben Sie das neue Kennwort erneut ein und drücken Sie die Eingabetaste.

Konfigurieren von BIOS-Starteinstellungen

Wenn Ihr Server mehrere Laufwerke aufweist, müssen Sie die BIOS-Einstellungen möglicherweise konfigurieren.

Die BIOS-Startkonfiguration legt fest, wie der Server gestartet wird. In der Regel wird zuerst das CD-ROM-Laufwerk aufgeführt.

HINWEIS Wenn Sie ESXi Embedded verwenden, legt die BIOS-Startkonfiguration fest, ob Ihr Server über das ESXi-Startgerät oder über ein anderes Startgerät gestartet wird. in der Regel erscheint das USB-Flashgerät an erster Stelle der BIOS-Starteinstellungen der Maschine, die ESXi hostet.

Sie können die Starteinstellung ändern, indem Sie die Startreihenfolge während des Starts im BIOS konfigurieren oder im Geräteauswahlmenü ein Startgerät auswählen. Wenn Sie im BIOS die Startreihenfolge ändern, wirkt sich die neue Einstellung auf alle nachfolgenden Neustartvorgänge aus. Wenn Sie ein Startgerät im Geräteeuswahlmenü auswählen, betrifft die Auswahl lediglich den aktuellen Startvorgang.

Einige Server haben kein Geräteeuswahl-Startmenü. In diesem Fall müssen Sie auch für einmalige Startvorgänge die Startreihenfolge im BIOS ändern und während eines nachfolgenden Neustarts wieder zurücksetzen.

Ändern der BIOS-Starteinstellungen für ESXi

Konfigurieren Sie die BIOS-Starteinstellung für ESXi, wenn Sie möchten, dass der Server standardmäßig ESXi startet.

ESXi Installable und ESXi Embedded dürfen sich nicht auf demselben Host befinden.

Vorgehensweise

1 Drücken Sie, während der ESXi-Host eingeschaltet wird, die entsprechende Taste, mit der Sie in das BIOS-Setup Ihrer Maschine gelangen.

   Abhängig von Ihrer Serverhardware ist dies eine Funktionstaste oder die ENTF-Taste. Die Option zum Starten des BIOS-Setup kann auf Ihrem Server unterschiedlich sein.

2 Wählen Sie die BIOS-Starteinstellung.

Option	Beschreibung
Wenn Sie die installierbare Version von ESXi verwenden	Wählen Sie die Festplatte aus, auf der Sie die ESXi-Software installiert haben, und verschieben Sie sie auf die erste Position in der Liste. Der Host startet mit ESXi.
Wenn Sie ESXi Embedded verwenden	Wählen Sie das USB-Flash-Gerät aus und verschieben Sie es an die erste Position in der Liste. Der Host wird im ESXi-Modus gestartet.

Konfigurieren der Starteinstellung für virtuelle Medien

Wenn Sie die Remoteverwaltungssoftware zum Einrichten von ESXi verwenden, müssen Sie möglicherweise die Starteinstellungen für virtuelle Medien konfigurieren.

Über virtuelle Medien kann ein Remotespeichermedium, wie z. B. eine CD-ROM, ein USB-Massenspeicher, ein ISO-Image und eine Diskette, mit einem Zielserver verbunden werden, der sich an einem beliebigen Ort im Netzwerk befinden kann. Der Zielserver hat Zugriff auf das Remotemedium und kann auf diesem lesen und schreiben, als wäre das Medium an den USB-Anschluss des Servers angeschlossen.

Voraussetzungen

ESXi Installable und ESXi Embedded dürfen sich nicht auf demselben Host befinden.

Vorgehensweise

1 Schließen Sie das Medium am virtuellen Gerät an.

  Wenn Sie beispielsweise einen Server von Dell benutzen, melden Sie sich am Dell Remote Access Controller (DRAC) oder einer ähnlichen Remoteverwaltungsschnittstelle an. Wählen Sie ein physisches Disketten- oder CD-ROM-Laufwerk aus oder geben Sie den Pfad zu einem Disketten- oder CD-ROM-Image an.

2 Starten Sie den Server neu.

3 Aktivieren Sie das Menü zur Geräteauswahl, während der Server eingeschaltet wird.

  Abhängig von Ihrer Serverhardware ist dies eine Funktionstaste oder die ENTF-Taste.

4 Befolgen Sie die Anweisungen zum Auswählen des virtuellen Geräts.

Der Server wird einmalig vom konfigurierten Gerät gestartet und wechselt bei anschließenden Starts zur standardmäßigen Startreihenfolge zurück.

Host kann nicht gestartet werden, nachdem Sie ESXi im UEFI-Modus installiert haben

Wenn Sie ESXi auf einer Hostmaschine im UEFI-Modus installieren, kann die Maschine möglicherweise nicht mehr gestartet werden.

Problem

Wenn Sie einen Neustart durchführen, nachdem Sie ESXi auf einer Hostmaschine im UEFI-Modus installiert haben, schlägt der Neustart möglicherweise fehl. In diesem Fall wird eine Fehlermeldung ähnlich der folgenden angezeigt: `Unerwarteter Netzwerkfehler. Kein Startgerät verfügbar.`

Ursache

Das Hostsystem erkennt nicht, dass die Festplatte, auf der ESXi installiert ist, das Startlaufwerk ist.

Lösung

1 Drücken Sie F11, während die Fehlermeldung auf dem Bildschirm angezeigt wird, um die Startoptionen anzuzeigen.

2 Wählen Sie eine Option ähnlich der folgenden aus: **Startoption hinzufügen**.

  Der Wortlaut der Option kann je nach System variieren.

3 Wählen Sie die Datei `\EFI\BOOT\BOOTx64.EFI` auf der Festplatte aus, auf der Sie ESXi installiert haben.

4 Ändern Sie die Startreihenfolge so, dass der Host anhand der Option, die Sie hinzugefügt haben, startet.

Netzwerkzugriff auf den ESXi -Host

Standardmäßig wird das ESXi-Verwaltungsnetzwerk mithilfe von DHCP konfiguriert. Nach Abschluss der Installation können Sie das Standardverhalten außer Kraft setzen und statische IP-Einstellungen für das Verwaltungsnetzwerk verwenden.

Tabelle 5-2. Netzwerkkonfigurationsszenarien, die von ESXi unterstützt werden

Szenario	Ansatz
Sie möchten die von DHCP konfigurierten IP-Einstellungen übernehmen.	Sie können in der direkten Konsole von ESXi die IP-Adresse finden, die der ESXi-Verwaltungsschnittstelle über DHCP zugewiesen wurde. Sie können diese IP-Adresse zum Herstellen einer Verbindung vom vSphere Web Client zum Host verwenden, um Einstellungen anzupassen, einschließlich des Änderns der Verwaltungs-IP-Adresse.
Eine der folgenden Aussagen trifft zu: ■ Sie verfügen nicht über einen DHCP-Server. ■ Der ESXi-Host ist nicht mit einem DHCP-Server verbunden. ■ Der angeschlossene DHCP-Server funktioniert nicht ordnungsgemäß.	Während der Autokonfigurationsphase wird eine Verbindungslokale IP-Adresse zugeteilt, die sich im Subnetz 169.254.x.x/16 befindet. Die zugewiesene IP-Adresse wird auf der direkten Konsole angezeigt. Sie können die Link-Local IP-Adresse durch Konfigurieren einer statischen IP-Adresse mithilfe der direkten Konsole außer Kraft setzen.
Der ESXi-Host ist mit einem funktionierenden DHCP-Server verbunden, aber Sie möchten die DHCP-konfigurierte IP-Adresse nicht verwenden.	Während der automatischen Konfigurationsphase weist die Software eine von DHCP konfigurierte IP-Adresse zu. Unter Verwendung der DHCP-konfigurierten Adresse können Sie die anfängliche Verbindung herstellen. Anschließend können Sie eine statische IP-Adresse konfigurieren. Wenn Sie physischen Zugriff auf den ESXi-Host haben, können Sie die DHCP-konfigurierte IP-Adresse außer Kraft setzen, indem Sie über die direkte Konsole eine statische IP-Adresse konfigurieren.
Ihre Sicherheitsrichtlinien lassen nicht das Einschalten unkonfigurierter Hosts im Netzwerk zu.	Befolgen Sie die Anweisungen in der Setup-Prozedur unter „Konfigurieren der Netzwerkeinstellungen auf einem Host, der mit dem Netzwerk nicht verbunden ist“, auf Seite 184.

Konfigurieren der Netzwerkeinstellungen auf einem Host, der mit dem Netzwerk nicht verbunden ist

In manchen hochsicheren Umgebungen dürfen im Netzwerk keine Hosts eingeschaltet werden, für die die Konfiguration aufgehoben wurde. Sie können den Host konfigurieren, bevor Sie den Host an das Netzwerk anschließen.

Voraussetzungen

Stellen Sie sicher, dass keine Netzwerkkabel mit dem Host verbunden sind.

Vorgehensweise

1 Schalten Sie den Host ein.

2 Verwenden Sie die Schnittstelle der direkten Konsole (DCUI), um das Kennwort für das Administratorkonto (root) zu konfigurieren.

3 Verwenden Sie die DCUI zum Konfigurieren einer statischen IP-Adresse.

4 Schließen Sie ein Netzwerkkabel an den Host an.

5 (Optional) Stellen Sie mit dem vSphere Web Client eine Verbindung zum vCenter Server-System her.

6 (Optional) Fügen Sie den Host zur vCenter Server-Bestandsliste hinzu.

Remoteverwaltung von ESXi

Sie können den vSphere Client, den vSphere Web Client und vCenter Server zum Verwalten Ihrer ESXi-Hosts verwenden.

Anleitungen zum Herunterladen und Installieren von vCenter Server und der vCenter Server-Komponenten oder zum Herunterladen und Bereitstellen der vCenter Server Appliance finden Sie unter Kapitel 8, „Installieren von vCenter Server auf einer virtuellen Windows-Maschine oder einem physischen Server“, auf Seite 247 und Kapitel 9, „Bereitstellen der vCenter Server Appliance“, auf Seite 259. Anweisungen zum Installieren des vSphere Client finden Sie unter „Installation vom vSphere-Client“, auf Seite 203.

Konfigurieren von Netzwerkeinstellungen

ESXi benötigt eine IP-Adresse für das Verwaltungsnetzwerk. Verwenden Sie den vSphere Web Client oder die direkte Konsole, um die grundlegenden Netzwerkeinstellungen zu konfigurieren.

Verwenden Sie den vSphere Web Client, wenn Sie mit der vom DHCP-Server zugewiesenen IP-Adresse zufrieden sind.

Verwenden Sie die direkte Konsole zur Netzwerkkonfiguration in den folgenden Fällen:

- Sie sind nicht mit der vom DHCP-Server zugewiesenen IP-Adresse zufrieden.
- Sie dürfen die vom DHCP-Server zugewiesene IP-Adresse nicht verwenden.
- ESXi hat keine IP-Adresse. Dieser Fall kann eintreten, wenn die Konfiguration von DHCP während der automatischen Konfigurationsphase fehlschlägt.
- Der falsche Netzwerkadapter wurde während der automatischen Konfigurationsphase ausgewählt.

ESXi-Netzwerksicherheitsempfehlungen

Die Isolierung des Netzwerkverkehrs ist entscheidend für eine sichere ESXi-Umgebung. Verschiedene Netzwerke erfordern verschiedenen Zugriff und verschiedene Isolierungsebenen.

Ihr ESXi-Host verwendet mehrere Netzwerke. Verwenden Sie angemessene Sicherheitsmaßnahmen für jedes Netzwerk und isolieren Sie Datenverkehr für bestimmte Anwendungen und Funktionen. Stellen Sie z. B. sicher, dass vSphere vMotion-Datenverkehr nicht über Netzwerke gesendet wird, in denen sich virtuelle Maschinen befinden. Durch Isolierung wird Snooping verhindert. Getrennte Netzwerke werden auch aus Leistungsgründen empfohlen.

- Netzwerke der vSphere-Infrastruktur werden für Funktionen wie VMware vSphere vMotion®, VMware vSphere Fault Tolerance und Speicher verwendet. Diese Netzwerke werden als für ihre spezifischen Funktionen isoliert betrachtet und oft nicht außerhalb eines einzelnen physischen Satzes von Serverracks geroutet.
- Ein Managementnetzwerk isoliert Datenverkehr des Clients, der Befehlszeilenschnittstelle oder der API sowie Datenverkehr von Drittsoftware von normalem Datenverkehr. Auf dieses Netzwerk dürfen nur System-, Netzwerk- und Sicherheits-Administratoren Zugriff haben. Verwenden Sie Jump-Box oder Virtual Private Network (VPN), um den Zugriff auf das Managementnetzwerk zu sichern. Kontrollieren Sie den Zugriff innerhalb dieses Netzwerks strikt auf mögliche Malware-Quellen.
- Der Datenverkehr von virtuellen Maschinen kann über ein oder zahlreiche Netzwerke fließen. Sie können die Isolierung von virtuellen Maschinen verbessern, indem Sie virtuelle Firewalllösungen einsetzen, in denen Firewallregeln beim virtuellen Netzwerkcontroller festgelegt werden. Diese Einstellungen werden zusammen mit der virtuellen Maschine migriert, wenn diese von einem Host zu einem anderen in der vSphere-Umgebung migriert.

Auswählen von Netzwerkadaptern für das Verwaltungsnetzwerk

Der Datenverkehr zwischen einem ESXi-Host und einer beliebigen externen Managementsoftware wird über einen Ethernet-Netzwerkadapter an den Host übertragen. Mit der direkten Konsole können Sie die Netzwerkadapter wählen, die vom Verwaltungsnetzwerk verwendet werden.

vCenter Server und der SNMP-Client sind Beispiele für externe Verwaltungssoftware. Netzwerkadapter auf dem Host heißen vmnic*N*, wobei N eine eindeutige Zahl ist, die den Netzwerkadapter identifiziert, z. B. vmnic0, vmnic1 usw.

Der ESXi-Host wählt während der Autokonfigurationsphase vmnic0 für den Verwaltungsverkehr. Sie können die Standardeinstellungen außer Kraft setzen, indem Sie manuell den Netzwerkadapter auswählen, der den Verwaltungsdatenverkehr des Hosts überträgt. In einigen Fällen kann es sinnvoll sein, einen Gigabit-Ethernet-Netzwerkadapter für den Verwaltungsdatenverkehr zu verwenden. Die Verfügbarkeit kann ebenfalls anhand der Auswahl mehrerer Netzwerkadapter sichergestellt werden. Die Verwendung mehrerer Netzwerkadapter ermöglicht Lastausgleich- und Failover-Funktionen.

Vorgehensweise

1. Wählen Sie in der direkten Konsole **Verwaltungsnetzwerk konfigurieren**, und drücken Sie die Eingabetaste.
2. Wählen Sie **Netzwerkadapter** aus, und drücken Sie die Eingabetaste.
3. Wählen Sie einen Netzwerkadapter aus und drücken Sie die Eingabetaste.

Sobald das Netzwerk funktionsfähig ist, können Sie den vSphere Web Client verwenden, um über vCenter Server eine Verbindung zum ESXi-Host herzustellen.

Festlegen der VLAN-ID

Sie können die ID des virtuellen LANs (VLAN-ID) für den ESXi-Host festlegen.

Vorgehensweise

1. Wählen Sie in der direkten Konsole **Verwaltungsnetzwerk konfigurieren**, und drücken Sie die Eingabetaste.
2. Wählen Sie **VLAN** und drücken Sie die Eingabetaste.
3. Geben Sie als VLAN-ID eine Zahl zwischen 1 und 4094 ein.

Konfigurieren von IP-Einstellungen für ESXi

DHCP legt standardmäßig die IP-Adresse, die Subnetzmaske und das Standard-Gateway fest.

Notieren Sie sich die IP-Adresse, falls Sie sie später wieder benötigen.

Damit DHCP funktionieren kann, benötigt Ihre Netzwerkumgebung einen DHCP-Server. Wenn DHCP nicht verfügbar ist, weist der Host die Link-Local IP-Adresse zu, die sich im Subnetz 169.254.x.x/16 befindet. Die zugewiesene IP-Adresse erscheint in der direkten Konsole. Wenn Sie nicht über physischen Zugriff auf den Host verfügen, können Sie über eine Remote-Managementanwendung auf die direkte Konsole zugreifen. Siehe „Verwenden von Anwendungen für die Remoteverwaltung“, auf Seite 54.

Wenn Sie über Zugriff auf die direkte Konsole verfügen, können Sie optional eine statische Netzwerkadresse konfigurieren. Die standardmäßige Subnetzmaske ist 255.255.0.0.

Konfigurieren der IP-Einstellungen von der direkten Konsole

Wenn Sie physischen Zugriff auf den Host oder Remotezugriff auf die direkte Konsole haben, können Sie die direkte Konsole verwenden, um die IP-Adresse, die Subnetzmaske und das Standard-Gateway zu konfigurieren.

Vorgehensweise

1 Wählen Sie **Verwaltungsnetzwerk konfigurieren** und drücken Sie die Eingabetaste.

2 Wählen Sie **IP-Konfiguration (IP Configuration)** aus, und drücken Sie die Eingabetaste.

3 Wählen Sie **Statische IP-Adresse und Netzwerkkonfiguration festlegen**.

4 Geben Sie die IP-Adresse, die Subnetzmaske und das Standard-Gateway ein und drücken Sie die Eingabetaste.

Konfigurieren der IP-Einstellungen im vSphere Web Client

Wenn Sie nicht über physischen Zugriff auf den Host verfügen, können Sie mit dem vSphere Web Client die statischen IP-Einstellungen konfigurieren.

Vorgehensweise

1 Melden Sie sich über vSphere Web Client beim vCenter Server an.

2 Wählen Sie den Host in der Bestandsliste aus.

3 Wählen Sie auf der Registerkarte **Verwalten** die Option **Netzwerk**.

4 Wählen Sie **Virtuelle Adapter**.

5 Wählen Sie **vmk0-Verwaltungsnetzwerk** und klicken Sie auf das Symbol „Bearbeiten“.

6 Wählen Sie **IPv4-Einstellungen**.

7 Wählen Sie **Statische IPv4-Einstellungen verwenden**.

8 Geben Sie die Einstellungen für die statische IPv4-Adresse ein oder ändern Sie sie.

9 (Optional) Legen Sie die statischen IPv6-Adressen fest.

   a Wählen Sie **IPv6-Einstellungen**.

   b Wählen Sie **Statische IPv6-Adressen**.

   c Klicken Sie auf das Symbol zum Hinzufügen.

   d Geben Sie die IPv6-Adresse ein und klicken Sie auf **OK**.

10 Klicken Sie auf **OK**.

Konfigurieren von DNS für ESXi

Sie können zwischen einer manuellen und einer automatischen DNS-Konfiguration des ESXi-Hosts wählen.

Standardmäßig wird eine automatische Konfiguration vorgenommen. Damit DNS funktionieren kann, benötigt Ihre Netzwerkumgebung einen DHCP-Server und einen DNS-Server.

In Netzwerkumgebungen, wo das automatische DNS nicht verfügbar oder nicht erwünscht ist, können Sie statische DNS-Informationen erstellen, einschließlich eines Hostnamens, eines primären und sekundären Namensservers sowie DNS-Suffixen.

Konfigurieren der DNS-Einstellungen von der direkten Konsole

Wenn Sie über physischen Zugriff auf den Host oder Remotezugriff auf die direkte Konsole verfügen, können Sie mit der direkten Konsole die DNS-Informationen konfigurieren.

Vorgehensweise

1 Wählen Sie **Verwaltungsnetzwerk konfigurieren** und drücken Sie die Eingabetaste.

2 Wählen Sie **DNS-Konfiguration (DNS Configuration)** aus, und drücken Sie die Eingabetaste.

3 Wählen Sie **Die folgenden DNS-Serveradressen und Hostnamen verwenden**.

4 Geben Sie den primären Server, einen alternativen Server (optional) und den Hostnamen ein.

Konfigurieren von DNS-Suffixen

Wenn Sie über physischen Zugriff auf den Host verfügen, können Sie die DNS-Informationen mit der direkten Konsole konfigurieren. DHCP ruft DNS-Suffixe standardmäßig ab.

Vorgehensweise

1 Wählen Sie in der direkten Konsole **Verwaltungsnetzwerk konfigurieren**.

2 Wählen Sie **Benutzerdefinierte DNS-Suffixe** aus, und drücken Sie die Eingabetaste.

3 Geben Sie neue DNS-Suffixe ein.

Testen des Verwaltungsnetzwerks

Über die direkte Konsole können Sie verschiedene einfache Netzwerkverbindungstests durchführen.

Die direkte Konsole führt die folgenden Tests durch.

- Senden des PING-Befehls an das Standard-Gateway
- Senden des PING-Befehls an den primären DNS-Namenserver
- Senden des PING-Befehls an den sekundären DNS-Namenserver
- Auflösen des konfigurierten Hostnamens

Vorgehensweise

1 Wählen Sie in der direkten Konsole **Verwaltungsnetzwerk testen**, und drücken Sie die Eingabetaste.

2 Drücken Sie die Eingabetaste, um den Test zu starten.

Neustarten von Verwaltungs-Agenten

Die Management-Agenten synchronisieren die VMware-Komponenten und ermöglichen Ihnen den Zugriff auf den ESXi-Host über vSphere Web Client und vCenter Server. Die Agenten werden mit der vSphere-Software installiert. Sie müssen die Verwaltungs-Agenten ggf. neu starten, wenn der Remotezugriff unterbrochen wird.

Beim Neustarten der Verwaltungs-Agenten werden alle Verwaltungs-Agenten und -dienste neu gestartet, die unter `/etc/init.d` auf dem ESXi-Host installiert und ausgeführt sind. Diese Agenten umfassen typischerweise zumeist hostd, ntpd, sfcbd, slpd, wsman, und vobd. Die Software startet auch den Fault Domain Manager (FDM) neu, falls dieser installiert ist.

Benutzer, die über vSphere Web Client oder vCenter Server auf diesen Host zugreifen, haben beim Neustarten der Verwaltungs-Agenten keine Verbindung mehr.

Vorgehensweise

1 Wählen Sie in der direkten Konsole **Fehlerbehebungsoptionen**, und drücken Sie die Eingabetaste.

2 Wählen Sie **Verwaltungs-Agenten neu starten** und drücken Sie die Eingabetaste.

3 Drücken Sie zur Bestätigung des Neustarts F11.

Der ESXi-Host startet die Management-Agenten und -dienste neu.

Neustarten des Verwaltungsnetzwerks

Ein Neustart der Verwaltungsnetzwerk-Schnittstelle ist möglicherweise erforderlich, um das Netzwerk wiederherzustellen oder eine DHCP-Lease zu erneuern.

Der Neustart des Verwaltungsnetzwerks hat einen kurzfristigen Netzwerkausfall zur Folge, der sich möglicherweise vorübergehend auf laufende virtuelle Maschinen auswirkt.

Wenn eine erneuerte DHCP-Lease in einer neuen Netzwerkidentität (IP-Adresse oder Hostname) resultiert, wird die Verbindung zur Remoteverwaltungssoftware getrennt.

Vorgehensweise

1 Wählen Sie in der direkten Konsole **Verwaltungsnetzwerk neustarten**, und drücken Sie die Eingabetaste.

2 Drücken Sie zur Bestätigung des Neustarts F11.

Wiederherstellen des Standard-Switches

Ein verteilter vSphere-Switch dient als einzelner virtueller Switch für alle verbundenen Hosts. Virtuelle Maschinen können eine konsistente Netzwerkkonfiguration beibehalten, wenn sie über mehrere Hosts hinweg migriert werden. Wenn Sie einen vorhandenen Standard-Switch oder virtuellen Adapter zu einem Distributed Switch migrieren und der Distributed Switch nicht mehr benötigt wird oder nicht mehr funktioniert, können Sie den Standard-Switch wiederherstellen, um sicherzustellen, dass der Zugriff auf den Host weiterhin gewährleistet ist.

Wenn Sie den Standard-Switch wiederherstellen, wird ein neuer virtueller Adapter erstellt und der aktuell mit dem verteilten Switch verbundene Verwaltungsnetzwerk-Uplink wird zum neuen virtuellen Switch migriert.

Aus folgenden Gründen kann das Wiederherstellen des Standard-Switches erforderlich sein:

- Der Distributed Switch wird nicht benötigt bzw. funktioniert nicht.
- Der Distributed Switch muss repariert werden, um die Konnektivität zu vCenter Server wiederherzustellen, und auf die Hosts muss weiterhin zugegriffen werden können.
- vCenter Server soll die Hosts nicht verwalten. Wenn der Host nicht mit vCenter Server verbunden ist, stehen die meisten Funktionen des verteilten Switches dem Host nicht mehr zur Verfügung.

Voraussetzungen

Stellen Sie sicher, dass Ihr Verwaltungsnetzwerk mit einem Distributed Switch verbunden ist.

Vorgehensweise

1 Wählen Sie aus der direkten Konsole die Option **Standard-Switch wiederherstellen** und drücken Sie die Eingabetaste.

   Befindet sich der Host auf einem Standard-Switch, steht diese Auswahl nicht zur Verfügung.

2 Drücken Sie zur Bestätigung F11.

Testen der Geräte- und Netzwerkkonnektivität

Über die direkte Konsole können Sie verschiedene einfache Netzwerkverbindungstests durchführen. Zusätzlich zum Verwaltungsnetzwerk können Sie auch andere Geräte und Netzwerke angeben.

Vorgehensweise

1 Wählen Sie in der direkten Konsole **Verwaltungsnetzwerk testen**, und drücken Sie die Eingabetaste.

2 Geben Sie Adressen zum Anpingen oder einen anderen aufzulösenden DNS-Hostnamen ein.

3 Drücken Sie die Eingabetaste, um den Test zu starten.

Speicherverhalten

Wenn Sie ESXi einschalten, wird der Host in eine Autokonfigurationsphase versetzt, während der die Systemspeichergeräte mit Standardwerten konfiguriert werden.

Wenn Sie nach der Installation des ESXi-Images den ESXi-Host neu starten, konfiguriert der Host die Systemspeichergeräte mit Standardwerten. Standardmäßig werden alle angezeigten leeren internen Festplatten mit VMFS formatiert, damit virtuelle Maschinen auf den Festplatten gespeichert werden können. In ESXi Embedded werden alle angezeigten leeren internen Festplatten ebenfalls standardmäßig mit VMFS formatiert.



Vorsicht ESXi überschreibt alle Festplatten, die leer erscheinen. Festplatten werden als leer betrachtet, wenn sie über keine gültigen Partitionstabellen oder Partitionen verfügen. Wenn Sie Software verwenden, die solche Festplatten einsetzt - vor allem, wenn Sie einen logischen Volume-Manager (LVM) anstelle von (oder zusätzlich zu) herkömmlichen Partitionsschemata verwenden, kann dies dazu führen, dass ESXi den lokalen LVM neu formatiert. Erstellen Sie vor dem erstmaligen Starten von ESXi zunächst eine Sicherung Ihrer Systemdaten.

Die Formatierungssoftware sorgt dafür, dass auf der Festplatte oder dem USB-Gerät, von dem der ESXi-Host gestartet wird, vorhandene, vom Hardwareanbieter erstellte Diagnosepartitionen beibehalten werden. Im restlichen Speicher erstellt die Software die Partitionen gemäß Tabelle 5-3.

Tabelle 5-3. Von ESXi auf dem Hostlaufwerk erstellte Partitionen

ESXi-Version	Erstellte Partitionen
ESXi Installable	Bei Neuinstallationen wird eine Reihe neuer Partitionen für Startoptionen, Scratch-Partition und Locker angelegt. Neue ESXi Installationen verwenden GUID-Partitionstabellen (GPT) anstatt der MSDOS basierten Partitionierung. Die Partitionstabelle selbst ist fester Bestandteil des Binär-Images und wird zum Installationszeitpunkt auf das Laufwerk geschrieben. Das ESXi Installationsprogramm hinterlässt die Scratch- und VMFS-Partitionen in leerem Zustand.ESXi erstellt diese Partitionen, wenn der Host nach Installation oder Upgrade zum ersten Mal gestartet wird. Eine 4-GB-VFATScratch-Partition wird für die Systemauslagerung erstellt. Siehe „Grundlegendes zur Scratch-Partition“, auf Seite 191. Die VFAT-Scratch-Partition wird nur auf der Festplatte erstellt, von der der ESXi-Host gestartet wird. **Hinweis** Zum Erstellen des VMFS-Volumes und einer Scratch-Partition in der Installation benötigt das ESXi-Installationsprogramm mindestens 5,2 GB an freiem Speicherplatz auf der Installationsfestplatte. Das Installationsprogramm hat nur Auswirkungen auf die Installationsfestplatte. Das Installationsprogramm wirkt sich nicht auf andere Festplatten des Servers aus. Wenn Sie auf einer Festplatte installieren, überschreibt das Installationsprogramm die gesamte Festplatte. Wenn das Installationsprogramm den Speicher automatisch konfiguriert, überschreibt es die Partitionen der Hardwareanbieter nicht. Während der ESXi-Installation wird eine 110 MB große Diagnosepartition für Core-Dumps erstellt.
ESXi Embedded	Eine Diagnosepartition mit 110 MB für Core-Dumps, wenn diese Partition nicht auf einer anderen Festplatte vorhanden ist. Die VFAT-Scratch- und Diagnosepartitionen werden nur auf der Festplatte erstellt, von der aus der ESXi-Host gestartet wird. Auf anderen Festplatten erstellt die Software eine VMFS5-Partition pro leerer Festplatte unter Verwendung der gesamten Festplatte. Es werden nur leere Festplatten formatiert.
ESXi Installable und ESXi Embedded	Eine VMFS5-Partition im restlichen freien Speicher.

Sie können dieses Standardverhalten außer Kraft setzen, wenn Ihre Richtlinie beispielsweise vorsieht, dass gemeinsam genutzter anstatt lokaler Speicher verwendet werden soll. Um die automatische Festplattenformatierung zu verhindern, trennen Sie die lokalen Speichergeräte unter folgenden Bedingungen vom Host:

- Bevor Sie den Host erstmalig starten.
- Bevor Sie den Host nach dem Zurücksetzen des Hosts auf die Standardwerte für die Konfiguration starten.

Zum Überschreiben der VMFS-Formatierung (wenn die automatische Festplattenformatierung bereits gestartet ist) können Sie den Datenspeicher entfernen. Informationen finden Sie in der Dokumentation *vCenter Server und Hostverwaltung*.

Grundlegendes zur Scratch-Partition

Während der automatischen Konfigurationsphase von neuen Installationen von ESXi wird eine 4 GB große VFAT-Scratch-Partition erstellt, sofern sich die Partition nicht auf einer anderen Festplatte befindet.

Hinweis Das Partitionieren von Hosts, für die ein Upgrade von ESXi-Versionen vor Version 5.0 auf ESXi 5.x durchgeführt wurde, unterscheidet sich erheblich vom Partitionieren neuer Installationen von ESXi 5.x. Informationen finden Sie in der Dokumentation *vSphere-Upgrade*.

Beim Starten von ESXi versucht das System zum Erstellen einer Scratch-Partition eine passende Partition auf einer lokalen Festplatte zu finden.

Die Scratch-Partition ist nicht erforderlich. Sie dient dem Speichern der Ausgabe von „vm-support“, die Sie benötigen, wenn Sie ein Supportpaket erstellen. Falls die Scratch-Partition nicht vorhanden ist, wird die Ausgabe von „vm-support“ auf einer Ramdisk gespeichert. Es ist bei knappem Arbeitsspeicher eventuell ratsam, eine Scratch-Partition zu erstellen, falls nicht bereits eine vorhanden ist.

Bei der installierbaren Version von ESXi wird die Partition während der Installation erstellt und ausgewählt. VMware empfiehlt, die Partition nicht zu ändern.

HINWEIS Zum Erstellen des VMFS-Volumes und der Scratch-Partition benötigt das ESXi-Installationsprogramm mindestens 5,2 GB an freiem Speicherplatz auf der Installationsfestplatte.

Wenn bei ESXi Embedded keine Partition gefunden wird, aber eine leere lokale Festplatte vorhanden ist, formatiert das System diese und erstellt eine Scratch-Partition. Wenn keine Scratch-Partition erstellt wird, können Sie eine konfigurieren. Eine Scratch-Partition ist aber nicht erforderlich. Sie können die Standardkonfiguration zudem außer Kraft setzen. Dies ist der Fall, wenn Sie eine Scratch-Partition in einem NFS-gemounteten Remoteverzeichnis erstellen möchten.

HINWEIS Das Installationsprogramm kann mehrere VFAT-Partitionen erstellen. Die Bezeichnung „VFAT“ bedeutet nicht immer, dass es sich um eine Scratch-Partition handelt. In einigen Fällen kann sich eine VFAT-Partition einfach Im Leerlauf befinden.

Festlegen der Scratch-Partition vom vSphere Web Client aus

Wenn keine Scratch-Partition festgelegt ist, sollten Sie eine konfigurieren, besonders wenn nicht genügend freier Arbeitsspeicher ein Problem werden könnte. Wenn keine Scratch-Partition vorhanden ist, wird die Ausgabe von „vm-support“ auf einer Ramdisk gespeichert.

Voraussetzungen

Das Verzeichnis, das für die Scratch-Partition verwendet wird, muss auf dem Host vorhanden sein.

Vorgehensweise

1. Stellen Sie vom vSphere Web Client aus eine Verbindung zu vCenter Server her.
2. Wählen Sie den Host in der Bestandsliste aus.
3. Klicken Sie auf die Registerkarte **Verwalten**.
4. Wählen Sie **Einstellungen**.
5. Wählen Sie **Erweiterte Systemeinstellungen**.

   Mit der Einstellung **ScratchConfig.CurrentScratchLocation** wird der aktuelle Speicherort der Scratch-Partition angegeben.
6. Geben Sie im Feld **ScratchConfig.ConfiguredScratchLocation** einen für diesen Host eindeutigen Verzeichnispfad ein.
7. Starten Sie den Host neu, damit die Änderungen wirksam werden.

Host wird beim Startvorgang unerwartet angehalten, wenn eine Startlaufwerk gemeinsam mit einem anderen Host verwendet wird

Wenn mehr als ein physischer oder virtueller Host von derselben gemeinsam genutzten physischen Festplatte oder LUN gestartet wird, können sie nicht dieselbe Scratch-Partition verwenden.

Problem

Der Host wird beim Startvorgang unerwartet angehalten, wenn eine Startlaufwerk gemeinsam mit einem anderen Host verwendet wird.

Ursache

Mehr als ein ESXi-Host kann dieselbe physische Festplatte oder LUN verwenden. Wenn für zwei solche Hosts dieselbe Scratch-Partition konfiguriert ist, können die Hosts möglicherweise nicht gestartet werden.

Lösung

1 Legen Sie fest, dass die Hosts nacheinander gestartet werden sollen, und starten Sie die Hosts.

   Mit dieser Einstellung können Sie die Hosts so starten, dass Sie die Scratch-Partition für einen von ihnen ändern können.

2 Stellen Sie vom vSphere Web Client aus eine Verbindung zu vCenter Server her.

3 Wählen Sie den Host in der Bestandsliste aus.

4 Klicken Sie auf die Registerkarte **Verwalten**.

5 Klicken Sie auf **Einstellungen**.

6 Klicken Sie unter „System“ auf **Erweiterte Systemeinstellungen**.

7 Wählen Sie **ScratchConfig**.

   Im Feld **ScratchConfig.CurrentScratchLocation** wird der aktuelle Speicherort der Scratch-Partition angegeben.

8 Geben Sie im Feld **ScratchConfig.ConfiguredScratchLocation** einen für diesen Host eindeutigen Verzeichnispfad ein.

9 Starten Sie den Host neu, damit die Änderungen wirksam werden.

Aktivieren von ESXi Shell- und SSH-Zugriff mit der Benutzerschnittstelle der direkten Konsole

Verwenden Sie die Benutzerschnittstelle der direkten Konsole zum Aktivieren der ESXi Shell.

Vorgehensweise

1 Drücken Sie in Direct Console User Interface die Taste F2, um das Menü für die Systemanpassung aufzurufen.

2 Wählen Sie **Fehlerbehebungsoptionen** und drücken Sie die Eingabetaste.

3 Wählen Sie im Menü „Optionen für den Fehlerbehebungsmodus“ einen Dienst aus, der aktiviert werden soll.

   - Aktivieren von ESXi Shell
   - Aktivieren von SSH

4 Drücken Sie die Eingabetaste, um den Dienst zu starten.

5 (Optional) Legen Sie die Zeitüberschreitung für ESXi Shell fest.

   Standardmäßig ist die Zeitüberschreitung für die ESXi Shell 0 (deaktiviert).

   Die Einstellung der Zeitüberschreitung für die Verfügbarkeit gibt die Anzahl der Minuten an, die verstreichen dürfen, bevor Sie sich nach der Aktivierung von ESXi Shell anmelden müssen. Wenn Sie sich nach Verstreichen dieses Zeitraums noch nicht angemeldet haben, wird die Shell deaktiviert.

   HINWEIS Wenn Sie zu diesem Zeitpunkt angemeldet sind, bleibt Ihre Sitzung bestehen. ESXi Shell wird jedoch deaktiviert, sodass sich keine anderen Benutzer anmelden können.

   ---

   a Wählen Sie im Menü „Optionen für den Fehlerbehebungsmodus“ die Option **ESXi Shell- und SSH-Zeitüberschreitungen ändern** aus und drücken Sie die Eingabetaste.

   b Geben Sie die Zeitüberschreitung für die Verfügbarkeit in Minuten ein.

      Die Einstellung der Zeitüberschreitung für die Verfügbarkeit gibt die Anzahl der Minuten an, die verstreichen dürfen, bevor Sie sich nach der Aktivierung der ESXi Shell anmelden müssen.

   c Drücken Sie die Eingabetaste.

   d Geben Sie den Zeitüberschreitungswert für die Leerlaufzeit ein.

      Der Zeitüberschreitungswert für die Leerlaufzeit gibt die Anzahl der Minuten an, die verstreichen darf, bis der Benutzer von interaktiven Sitzungen, die sich im Leerlauf befinden, abgemeldet wird. Änderungen an den Zeitüberschreitungswerten für die Leerlaufzeit werden erst wirksam, wenn Sie sich das nächste Mal bei der ESXi Shell anmelden. Sie gelten nicht für aktuelle Sitzungen.

6 Drücken Sie die Esc-Taste wiederholt, bis Sie zurück zum Hauptmenü der Benutzerschnittstelle der direkten Konsole gelangt sind.

Anzeigen von Systemprotokollen

Systemprotokolle enthalten detaillierte Informationen zu Ereignissen während des Systembetriebs.

Vorgehensweise

1 Wählen Sie in der direkten Konsole **Systemprotokolle anzeigen (View System Logs)**.

2 Drücken Sie zum Anzeigen eines bestimmten Protokolls die entsprechende Taste.

   vCenter Server-Agent-Protokolle (vpxa) werden angezeigt, wenn Sie den Host zu vCenter Server hinzufügen.

3 Drücken Sie die Eingabe- oder Leertaste, um die Meldungen zu durchlaufen.

4 Führen Sie eine Suche mithilfe eines regulären Ausdrucks durch.

   a Drücken Sie die Schrägstrichtaste (/).

   b Geben Sie den zu suchenden Text ein.

   c Drücken Sie die Eingabetaste.

   Der gefundene Text wird auf dem Bildschirm hervorgehoben.

5 Drücken Sie „q“, um zur direkten Konsole zurückzukehren.

Weiter

Siehe auch „Konfiguration von Syslog auf ESXi-Hosts“, auf Seite 195.

Konfiguration von Syslog auf ESXi -Hosts

Auf allen ESXi-Hosts wird ein syslog-Dienst (`vmsyslogd`) ausgeführt, der Meldungen vom VMkernel und anderen Systemkomponenten in Protokolldateien ablegt.

Sie können den vSphere Web Client oder den vCLI-Befehl `esxcli system syslog` zum Konfigurieren des syslog-Dienstes verwenden.

Weitere Informationen zur Verwendung von vCLI-Befehlen finden Sie unter *Erste Schritte mit vSphere-Befehlszeilenschnittstellen*.

Vorgehensweise

1 Wählen Sie den Host im Bestandslistenbereich des vSphere Web Client aus.

2 Klicken Sie auf die Registerkarte **Verwalten**.

3 Klicken Sie im Bereich „System“ auf **Erweiterte Einstellungen**.

4 Suchen Sie den Bereich **Syslog** in der Liste „Erweiterte Systemeinstellungen“.

5 Um das Protokollieren global einzurichten, wählen Sie die zu ändernde Einstellung aus und klicken Sie auf das Symbol „Bearbeiten“.

Option	Beschreibung
Syslog.global.defaultRotate	Legt die maximale Anzahl der beizubehaltenden Archive fest. Sie können diese Anzahl global und für einzelne Unterprotokollierer festlegen.
Syslog.global.defaultSize	Legt die Standardgröße des Protokolls in KB fest, bevor das System eine Rotation der Protokolle durchführt. Sie können diese Anzahl global und für einzelne Unterprotokollierer festlegen.
Syslog.global.LogDir	Verzeichnis, in dem Protokolle gespeichert werden. Das Verzeichnis kann sich auf gemounteten NFS- oder VMFS-Volumes befinden. Nur das Verzeichnis `/scratch` auf dem lokalen Dateisystem bleibt nach einem Neustart konsistent. Das Verzeichnis sollte das Format [*Datenspeichername*] *Pfad_zur_Datei* aufweisen, wobei sich der Pfad auf das Stammverzeichnis des Volumes bezieht, in dem sich das Backing für den Datenspeicher befindet. Beispielsweise ist der Pfad `[storage1] /systemlogs` dem Pfad `/vmfs/volumes/storage1/systemlogs` zuzuordnen.
Syslog.global.logDirUnique	Durch die Auswahl dieser Option wird ein Unterverzeichnis mit dem Namen des ESXi-Hosts im von **Syslog.global.LogDir** angegebenen Verzeichnis erstellt. Ein eindeutiges Verzeichnis ist nützlich, wenn dasselbe NFS-Verzeichnis von mehreren ESXi-Hosts verwendet wird.
Syslog.global.LogHost	Remotehost, mit dem Syslog-Meldungen weitergeleitet werden, und Port, auf dem der Remotehost Syslog-Meldungen empfängt. Sie können das Protokoll und den Port einbeziehen, z. B. `ssl://Hostname1:1514`. UDP (Standard), TCP und SSL werden unterstützt. Beim Remotehost muss syslog installiert und ordnungsgemäß konfiguriert sein, damit die weitergeleiteten Syslog-Meldungen empfangen werden. Weitere Informationen zur Konfiguration finden Sie in der Dokumentation zum auf dem Remotehost installierten syslog-Dienst.

6 (Optional) So überschreiben Sie die Standardprotokollgröße und die Rotationsangaben für ein Protokoll.

   a Klicken Sie auf den Namen des Protokolls, das Sie anpassen möchten.

   b Klicken Sie auf das Symbol „Bearbeiten“ und geben Sie die Anzahl der Rotationen und die Protokollgröße an, die Sie verwenden möchten.

7 Klicken Sie auf **OK**.

Änderungen an der syslog-Option werden sofort wirksam.

Konfigurieren der Protokollfilterung auf ESXi -Hosts

Mithilfe der Protokollfilterung können Sie die Protokollierungsrichtlinie des Syslog-Diensts ändern, der auf einem ESXi-Host ausgeführt wird. Sie können Protokollfilter erstellen, um die Anzahl doppelter Einträge in den ESXi-Protokollen zu reduzieren und bestimmte Protokollereignisse komplett auf eine schwarze List (Blacklist) zu setzen.

Protokollfilter betreffen alle Protokollereignisse, die vom vmsyslogd-Daemon des ESXi-Hosts verarbeitet werden, und zwar unabhängig davon, ob sie in einem Protokollverzeichnis oder auf einem Remote-Syslog-Server aufgezeichnet werden.

Beim Erstellen eines Protokollfilters legen Sie die maximale Anzahl von Protokolleinträgen für die Protokollmeldungen fest, die von einer oder mehreren angegebenen Systemkomponenten generiert werden und mit einer bestimmten Zeichenfolge übereinstimmen. Sie müssen die Protokollfilterungsfunktion aktivieren und den Syslog-Daemon erneut laden, um die Protokollfilter auf dem ESXi-Host zu aktivieren.

Wichtig Wenn Sie einen Grenzwert für den Umfang der Protokollierungsinformationen festlegen, können Sie potenzielle Systemfehler möglicherweise nicht ordnungsgemäß beheben. Wenn nach Erreichen der maximalen Anzahl von Protokolleinträgen eine Protokollrotation erfolgt, verlieren Sie möglicherweise alle Instanzen einer gefilterten Nachricht.

Vorgehensweise

1. Melden Sie sich bei der ESXi-Shell als Root-Benutzer an.

2. Fügen Sie in der Datei `/etc/vmware/logfilters` den folgenden Eintrag hinzu, um einen neuen Protokollfilter zu erstellen.

   ```
   numLogs | ident | logRegexp
   ```

   wobei:

   - *numLogs* legt die maximale Anzahl von Protokolleinträgen für die angegebenen Protokollmeldungen fest. Nach Erreichen dieses Werts werden die angegebenen Protokollmeldungen gefiltert und ignoriert. Verwenden Sie den Wert **`0`**, um alle angegebenen Protokollmeldungen zu filtern und zu ignorieren.

   - *ident* gibt eine oder mehrere Systemkomponenten an, um den Filter auf die Protokollmeldungen anzuwenden, die von diesen Komponenten generiert werden. Informationen zu den Systemkomponenten, die Protokollmeldungen generieren, finden Sie in den Werten der `idents`-Parameter in den Syslog-Konfigurationsdateien, die im Verzeichnis `/etc/vmsyslog.conf.d` gespeichert sind. Verwenden Sie eine kommagetrennte Liste, um einen Filter auf mehrere Systemkomponenten anzuwenden. Verwenden Sie **`*`**, um einen Filter auf alle Systemkomponenten anzuwenden.

   - *logRegexp* bezeichnet eine Zeichenfolge unter Beachtung der Groß-/Kleinschreibung mit Python-Syntax für reguläre Ausdrücke, um die Protokollmeldungen anhand ihres Inhalts zu filtern.

   Wenn Sie beispielsweise einen Grenzwert von maximal zwei Protokolleinträgen für die hostd-Komponente für Meldungen festlegen möchten, die der Zeichenfolge `SOCKET connect failed, error 2: No such file or directory` mit einer beliebigen Fehlerzahl entsprechen, fügen Sie den folgenden Eintrag hinzu:

   ```
   2 | hostd | SOCKET connect failed, error .*: No such file or directory
   ```

   Hinweis Eine Zeile, die mit `#` beginnt, bezeichnet einen Kommentar. Die restliche Zeile wird in diesem Fall ignoriert.

   ---

3 Fügen Sie in der Datei `/etc/vmsyslog.conf` den folgenden Eintrag hinzu, um die Protokollfilterungsfunktion zu aktivieren.

```
enable_logfilters = true
```

4 Führen Sie den Befehl `esxcli system syslog reload` aus, um den Syslog-Daemon erneut zu laden und die Konfigurationsänderungen anzuwenden.

Festlegen der Akzeptanzebene des Host-Image-Profils

Die Akzeptanzebene des Host-Image-Profils legt fest, welche vSphere-Installationspakete (VIBs) für die Installation akzeptiert werden.

VIB-Signaturen werden auf Basis einer Kombination aus VIB-Akzeptanzebene und Akzeptanzebene des Host-Image-Profils für die Installation geprüft und akzeptiert. VIBs werden mit einer Akzeptanzebene versehen, die ihrem Signaturstatus abhängt.

Siehe „Akzeptanzebenen“, auf Seite 154.

Voraussetzungen

Erforderliche Rechte: **Host.Konfiguration.Sicherheitsprofil** und **Host.Konfiguration.Firewall**

Vorgehensweise

1 Stellen Sie vom vSphere Web Client aus eine Verbindung zu vCenter Server her.

2 Wählen Sie den Host in der Bestandsliste aus.

3 Klicken Sie auf die Registerkarte **Verwalten**.

4 Klicken Sie auf **Einstellungen**.

5 Klicken Sie unter „System“ auf **Sicherheitsprofil**.

6 Führen Sie einen Bildlauf nach unten zu „Akzeptanzebene des Host-Image-Profils“ durch, und klicken Sie auf **Bearbeiten**.

7 Wählen Sie die Akzeptanzebene aus und klicken Sie auf **OK**.

Tabelle 5-4. Akzeptanzebenen des Host-Image-Profils

Akzeptanzebene des Host-Image-Profils	Akzeptierte Ebenen der VIBs
VMware Certified	VMware Certified
VMware Accepted	VMware Certified, VMware Accepted
Unterstützte Partner	VMware Certified, VMware Accepted, Unterstützte Partner
Unterstützte Community	VMware Certified, VMware Accepted, Unterstützte Partner, Unterstützte Community

Zurücksetzen der Systemkonfiguration

Wenn bei der Ermittlung der Ursache eines Problems mit Ihrem ESXi-Host Schwierigkeiten auftreten, können Sie die Systemkonfiguration zurücksetzen.

Änderungen an der Systemkonfiguration können mit verschiedenen Problemen zusammenhängen, z. B. mit Problemen mit der Konnektivität zu Netzwerk und Geräten. Durch Zurücksetzen der Systemkonfiguration lassen sich diese Probleme möglicherweise beheben. Wenn sich das Problem durch Zurücksetzen der Systemkonfiguration nicht beheben lässt, können weiterhin Konfigurationsänderungen als Problemursache ausgeschlossen werden, die seit der erstmaligen Einrichtung vorgenommen wurden.

Wenn Sie die Konfiguration zurücksetzen, werden alle Ihre Konfigurationsänderungen außer Kraft gesetzt, das Kennwort des Administratorkontos (root) gelöscht und der Host neu gestartet. Von Ihrem Hardwareanbieter vorgenommene Konfigurationsänderungen, z. B. IP-Adresseneinstellungen und Lizenzkonfiguration, könnten möglicherweise auch gelöscht werden.

Durch das Zurücksetzen der Konfiguration werden auf dem ESXi-Host keine virtuelle Maschinen entfernt. Nach dem Zurücksetzen der Konfiguration sind die virtuelle Maschinen nicht sichtbar. Sie können sie jedoch wieder sichtbar machen, indem Sie den Speicher neu konfigurieren und die virtuelle Maschinen neu registrieren.



VORSICHT Für Benutzer, die auf den Host zugreifen, geht die Verbindung verloren, wenn Sie die Konfiguration zurücksetzen.

Voraussetzungen

Sichern Sie Ihre ESXi-Konfiguration, bevor Sie die Konfiguration zurücksetzen, falls Sie sie wiederherstellen möchten.

Vorgehensweise

1 Verwenden Sie den vSphere CLI-Befehl `vicfg-cfgbackup`, um die Konfiguration zu sichern.

2 Wählen Sie in der direkten Konsole die Option **Systemkonfiguration zurücksetzen** und drücken Sie die Eingabetaste.

3 Drücken Sie zur Bestätigung F11.

Das System startet neu, nachdem alle Einstellungen auf die Standardwerte zurückgesetzt wurden.

Entfernen aller benutzerdefinierten Pakete auf ESXi

Sie können hinzugefügte benutzerdefinierte Pakete auch entfernen.

Voraussetzungen

Bevor Sie benutzerdefinierte Pakete entfernen, fahren Sie gestartete virtuelle Maschinen herunter oder migrieren Sie sie vom ESXi-Host.

Vorgehensweise

1 Starten Sie den ESXi-Host neu.

2 Wählen Sie in der direkten Konsole **Benutzerdefinierte Erweiterungen entfernen** aus und drücken Sie F11, um Ihre Auswahl zu bestätigen.

3 Starten Sie den Host neu.

Alle benutzerdefinierten Pakete werden entfernt.

Deaktivieren der Unterstützung für Nicht-ASCII-Zeichen in Namen von Dateien und Verzeichnissen virtueller Maschinen

Standardmäßig unterstützt ESXi die Verwendung von Nicht-ASCII-Zeichen für Datei- und Verzeichnisnamen virtueller Maschinen. Sie können diese Unterstützung deaktivieren, indem Sie die Datei `/etc/vmware/hostd/config.xml` bearbeiten.

Nachdem Sie diese Unterstützung deaktiviert haben, können Sie weiterhin Nicht-ASCII-Zeichen für die Namen virtueller Maschinen eingeben. In den vSphere-Benutzeroberflächen werden die VM-Namen in den Nicht-ASCII-Zeichen angezeigt, ESXi konvertiert jedoch die tatsächlichen Datei- und Verzeichnisnamen in ASCII-Zeichenfolgen.

Vorgehensweise

1 Öffnen Sie mit einem Texteditor die Datei `/etc/vmware/hostd/config.xml` für den ESXi-Host.

2 Fügen Sie innerhalb des Tags `<config></config>` den folgenden Code hinzu.

```
<g11nSupport>false</g11nSupport>
```

3 Speichern und schließen Sie die Datei.

4 Starten Sie den Host neu.

Außerbetriebnahme eines ESXi -Hosts

Wenn Ihr Server nicht als ESXi-Host dienen soll, können Sie die ESXi-Hostmaschine außer Betrieb nehmen.

Vorgehensweise

1 Entfernen Sie VMFS-Datenspeicher von den internen Festplatten, sodass diese nicht mehr für die Speicherung virtueller Maschinen eingerichtet sind.

2 Ändern Sie die Starteinstellung im BIOS, sodass der Host nicht mehr im ESXi-Modus gestartet wird.

3 Installieren Sie ein anderes Betriebssystem.

Nach der Installation und Einrichtung von ESXi

6

Nachdem ESXi installiert und eingerichtet wurde, können Sie über den vSphere Web Client und vCenter Server den Host verwalten und lizenzieren und Ihre ESXi-Konfiguration sichern.

Sie können auch den vSphere Client verwenden, um eine direkte Verbindung mit dem ESXi-Host herstellen.

Dieses Kapitel behandelt die folgenden Themen:

Verwalten des ESXi -Hosts

Der vSphere Client bietet die einfachste Möglichkeit, Ihren ESXi-Host zu verwalten und dessen virtuelle Maschinen zu betreiben.

Sie können auch mit dem vSphere Web Client über einen Webbrowser eine Verbindung zu vCenter Server herstellen und diesen verwalten. Der vSphere Web Client wird zusammen mit vCenter Server und der vCenter Server Appliance installiert, und Sie können ihn zum Verwalten Ihrer ESXi-Hosts verwenden.

Lizenzieren von ESXi -Hosts

Nach der Installation von ESXi haben Sie 60 Tage Zeit, den gesamten vSphere-Funktionsumfang der vSphere Enterprise Plus-Lizenz auszuprobieren. Sie müssen dem Host eine entsprechende Lizenz zuweisen, bevor der Testzeitraum abläuft.

Die Lizenzierung von ESXi-Hosts erfolgt über vSphere-Lizenzen mit Kapazität pro CPU. Zur korrekten Lizenzierung von Hosts müssen Sie ihnen eine vSphere-Lizenz mit genügend CPU-Kapazität zuweisen, um alle CPUs in den Hosts abzudecken. Die Lizenz muss alle vom Host verwendeten Funktionen unterstützen. Wenn die Hosts beispielsweise mit einem vSphere Distributed Switch verbunden sind, muss die zugewiesene Lizenz vSphere Distributed Switches unterstützen.

Zur Lizenzierung von ESXi-Hosts stehen Ihnen folgende Methoden zur Verfügung:

- Gleichzeitige Lizenzierung mehrerer Hosts über die Lizenzverwaltungsfunktion in vSphere Web Client: Die Hosts müssen mit einem vCenter Server-System verbunden sein. Weitere Informationen finden Sie unter *vCenter Server und Hostverwaltung*.
- Massenlizenzierung mithilfe von PowerCLI-Befehlen: Die Massenlizenzierung kann auf allen ESXi-Hosts eingesetzt werden, ist jedoch besonders nützlich für mit Auto Deploy bereitgestellte Hosts. Siehe „Einrichten der Massenlizenzierung", auf Seite 91.
- Lizenzierung einzelner ESXi-Hosts über eine Direktverbindung mit dem vSphere Client: Weitere Informationen finden Sie unter *vSphere-Verwaltung mit dem vSphere Client*.

Grundlegendes zum ESXi -Testmodus und -Lizenzmodus

Mit dem Testmodus können Sie alle Funktionen von ESXi-Hosts kennenlernen. Im Testmodus sind die gleichen Funktionen wie mit einer vSphere Enterprise Plus-Lizenz verfügbar. Vor Ablauf des Testmodus müssen Sie Ihren Hosts eine Lizenz zuweisen, die alle genutzten Funktionen unterstützt.

Beispielsweise können Sie im Testmodus vSphere vMotion-Technologie, die vSphere HA-Funktion, die vSphere DRS-Funktion und andere Funktionen nutzen. Wenn Sie diese Funktionen weiter nutzen möchten, müssen Sie ihnen eine Lizenz zuweisen, die sie unterstützt.

Die installierbare Version von ESXi-Hosts wird immer im Testmodus installiert. ESXi Embedded wird von Ihrem Hardwareanbieter auf einem internen Speichergerät vorinstalliert. Es ist möglicherweise im Testmodus oder vorlizenziert.

Die Testperiode beträgt 60 Tage und beginnt mit dem Einschalten des ESXi-Host. Während der 60-tägigen Testphase können Sie jederzeit vom lizenzierten Modus in den Testmodus wechseln. Die in der Testperiode verfügbare Zeit wird um die bereits genutzte Zeit reduziert.

Angenommen, Sie haben einen ESXi-Host im Testmodus bereits seit 20 Tagen verwendet und weisen dann dem Host einen vSphere Standard Edition-Lizenzschlüssel zu. Wenn Sie den Host auf den Testmodus zurücksetzen, können Sie alle Funktionen des Hosts während der verbleibenden 40 Tage im Testmodus nutzen.

Informationen zur Lizenzierung für ESXi-Hosts finden Sie in der Dokumentation *vCenter Server und Hostverwaltung*.

Notieren des Lizenzschlüssels eines ESXi -Hosts

Sie sollten sich den Lizenzschlüssel für den Fall notieren, dass auf einen Host nicht zugegriffen oder dieser nicht gestartet werden kann. Sie können den Lizenzschlüssel aufschreiben und auf dem Server festkleben oder ihn an einem sicheren Ort aufbewahren. Sie können von der Benutzerschnittstelle der direkten Konsole oder vom vSphere Web Client aus auf den Lizenzschlüssel zugreifen.

Anzeigen der Lizenzschlüssel von ESXi -Hosts vom vSphere Web Client aus

Sie können die Lizenzschlüssel der Hosts, die mit einem vCenter Server-System verbunden sind, über den vSphere Web Client anzeigen.

Vorgehensweise

1. Wählen Sie im vSphere Web Client die Option **Verwaltung** aus.
2. Wählen Sie unter „Lizenzierung“ die Option **Lizenzen** aus.
3. Wählen Sie auf der Registerkarte **Assets** die Option **Hosts** aus.
4. Klicken Sie in der Spalte „Lizenz“ auf eine Lizenz.

Sie können Informationen zur Lizenz anzeigen, zum Beispiel ihre Nutzung und den Lizenzschlüssel.

Zugriff auf den ESXi-Lizenzschlüssel von der direkten Konsole aus

Wenn Sie über physischen Zugriff auf den Host oder Remotezugriff auf die direkte Konsole verfügen, können Sie mit der direkten Konsole auf den ESXi-Lizenzschlüssel zugreifen.

Vorgehensweise

- Wählen Sie in der direkten Konsole **Support-Informationen anzeigen**.

  Der Lizenzschlüssel erscheint im Format „XXXXX-XXXXX-XXXXX-XXXXX-XXXXX“ und wird als Lizenz-Seriennummer bezeichnet.

  HINWEIS Die Seriennummer der physischen Maschine erscheint auch und wird als Seriennummer bezeichnet. Verwechseln Sie den Lizenzschlüssel nicht mit der Seriennummer der physischen Maschine.

Installation vom vSphere-Client

Über den vSphere-Client können Sie eine Verbindung mit dem ESXi-Host herstellen.

Voraussetzungen

- Stellen Sie sicher, dass Ihnen das Installationsprogramm für vCenter Server oder für den vSphere-Client zur Verfügung steht.
- Stellen Sie sicher, dass Sie Mitglied der Administratorgruppe auf diesem System sind.
- Stellen Sie sicher, dass das System über einen Internetzugang verfügt.

Vorgehensweise

1 Führen Sie das vSphere-Client-Installationsprogramm wie folgt aus.

Option	Beschreibung
Wenn Sie vom vCenter Server-Installationsprogramm aus installieren	a Doppelklicken Sie im Softwareinstallationsverzeichnis auf die Datei `autorun.exe`. b Wählen Sie **vSphere™-Client**. c Klicken Sie auf **Install**.
Wenn Sie den vSphere-Client heruntergeladen haben	Doppelklicken Sie auf die Datei `VMware-viclient-`*`Build-Nummer`*`.exe`.

2 Folgen Sie den Eingabeaufforderungen des Assistenten, um die Installation abzuschließen.

Mit dem vSphere-Client können Sie eine Verbindung zu einem ESXi-Host oder zu einem vCenter Server-System herstellen.

Vor der Installation von vCenter Server oder der Bereitstellung der vCenter Server Appliance

7

Sie können vCenter Server auf einem physischen System oder einer virtuellen Maschine installieren, die auf einem ESXi-Host ausgeführt wird. Darüber hinaus können Sie die vCenter Server Appliance herunterladen und auf einem ESXi-Host der Version 5.0 oder höher oder aber auf einer vCenter Server-Instanz der Version 5.0 oder höher bereitstellen.

Dieses Kapitel behandelt die folgenden Themen:

Vorbereiten der vCenter Server-Datenbanken

vCenter Server benötigt eine Datenbank zum Speichern und Organisieren von Serverdaten. Sie können entweder die mitgelieferte PostgreSQL-Datenbank verwenden, die bei der Bereitstellung installiert und konfiguriert werden kann, oder Sie können eine externe Datenbank einrichten.

vCenter Server für Windows unterstützt Oracle- und Microsoft SQL-Datenbanken, während die vCenter Server Appliance nur eine Oracle-Datenbank als externe Datenbank unterstützt.

Die Datenbank wird zwar automatisch vom Installationsprogramm konfiguriert, aber Sie können eine externe Datenbank manuell oder mithilfe eines Skripts konfigurieren. Darüber hinaus benötigt der DSN-Benutzer bestimmte Berechtigungen.

Siehe „Festlegen von Datenbankberechtigungen durch das manuelle Erstellen von Datenbankrollen und des VMW-Schemas", auf Seite 210 und „Konfigurieren eines Oracle-Datenbankbenutzers", auf Seite 220.

Die Datenbankkennwörter werden auf der virtuellen Windows-Maschine oder dem physischen Host, auf der/dem Sie vCenter Server installieren, und in der vCenter Server Appliance als lesbarer Text gespeichert. Die Dateien mit den Kennwörtern sind durch das Betriebssystem geschützt, d. h., nur ein lokaler Windows-Administrator oder ein Linux-Root-Benutzer kann auf diese Dateien zugreifen und sie lesen.

vCenter Server-Instanzen können nicht dasselbe Datenbankschema verwenden. Mehrere vCenter Server-Datenbanken können sich auf demselben Datenbankserver befinden oder auf mehrere Datenbankserver aufgeteilt werden. Für Oracle-Datenbanken, die das Schemaobjektkonzept verwenden, können Sie mehrere vCenter Server-Instanzen auf einem einzelnen Datenbankserver ausführen, wenn für jede vCenter Server-Instanz ein anderer Schemabesitzer vorhanden ist. Darüber hinaus können Sie für jede vCenter Server-Instanz einen dedizierten Oracle-Datenbankserver verwenden.

Es ist nicht möglich, vCenter Server zu installieren und auf eine ältere externe vCenter Server-Datenbank zu verweisen. Ein Upgrade der vCenter Server 5.x-Datenbank auf die neueste Version ist nur möglich, wenn Sie für die mit dieser Datenbank verbundenen vCenter Server-Instanz ein Upgrade durchführen. Weitere Informationen zum Upgrade von vCenter Server finden Sie unter *vSphere-Upgrade*.

Konfigurationshinweise für die vCenter Server -Datenbank

Vergewissern Sie sich, sobald Sie einen Datenbanktyp ausgewählt haben, dass Sie mit allen speziellen Konfigurationsanforderungen vertraut sind.

Tabelle 7-1 ist keine vollständige Liste der für vCenter Server und vCenter Server Appliance unterstützten Datenbanken. Weitere Informationen zu bestimmten Datenbankversionen und Service Pack-Konfigurationen, die von vCenter Server unterstützt werden, finden Sie in der VMware-Produkt-Interoperabilitätsmatrix. Die vCenter Server Appliance unterstützt die gleichen Oracle-Datenbankversionen wie vCenter Server. Nur besondere Datenbankkonfigurationshinweise, die in den Produktinteroperatbilitätstabellen nicht aufgeführt sind, werden in Tabelle 7-1 bereitgestellt.

vCenter Server-Datenbanken erfordern einen UTF-Codesatz.

Wenden Sie sich an Ihren Datenbankadministrator, um die jeweiligen Anmeldeinformationen für die Datenbank zu erhalten.

Tabelle 7-1. Konfigurationshinweise für von vCenter Server unterstützte Datenbanken

Datenbanktyp	Konfigurationshinweise
PostgreSQL	Für vCenter Server 6.0 ist die mitgelieferte PostgreSQL-Datenbank für Umgebungen mit bis zu 20 Hosts und bis zu 200 virtuellen Maschinen geeignet. Für die vCenter Server Appliance können Sie die eingebettete PostgreSQL-Datenbank für Umgebungen mit bis zu 1000 Hosts und bis zu 10.000 virtuellen Maschinen verwenden. **Wichtig** Wenn Sie die eingebettete PostgreSQL-Datenbank verwenden, wird bei der Deinstallation von vCenter Server unter Windows auch die eingebettete Datenbank deinstalliert, und alle Daten gehen verloren.
Microsoft SQL Server 2008 R2 SP2 oder höher	Stellen Sie sicher, dass die Maschine einen gültigen ODBC-Namen der Datenquelle (Data Source Name, DSN) hat. **Hinweis** vCenter Server Appliance unterstützt diese Datenbank nicht.
Microsoft SQL Server 2012	Stellen Sie sicher, dass die Maschine einen gültigen ODBC-Namen der Datenquelle (Data Source Name, DSN) hat. **Hinweis** vCenter Server Appliance unterstützt diese Datenbank nicht.
Microsoft SQL Server 2014	Stellen Sie sicher, dass die Maschine einen gültigen ODBC-Namen der Datenquelle (Data Source Name, DSN) hat. **Hinweis** vCenter Server Appliance unterstützt diese Datenbank nicht.
Oracle 11g und Oracle 12c	Stellen Sie sicher, dass die Maschine einen gültigen ODBC-Namen der Datenquelle (Data Source Name, DSN) hat. Wenden Sie nach Abschluss der Installation von vCenter Server den neuesten Patch auf den Oracle-Client und -Server an.

Erstellen eines 64-Bit-DSN

Für das vCenter Server-System ist ein 64-Bit-DSN erforderlich. Diese Anforderung gilt für alle unterstützten Datenbanken.

HINWEIS Ihre SQL-Datenbank stellt möglicherweise bestimmte Anforderungen an den ODBC-Treiber. Weitere Informationen hierzu finden Sie im Knowledgebase-Artikel 1015804.

Vorgehensweise

1 Wählen Sie im Windows-Startmenü **Systemsteuerung > Verwaltung > Datenquellen (ODBC)** aus.

2 Erstellen Sie einen System-DSN.

Wenn Sie eine Microsoft SQL-Datenbank verwenden, erstellen Sie den System-DSN mit dem SQL Native Client, Version 10 oder 11.

3 Testen Sie die Verbindung.

Das System verfügt nun über einen DSN, der zu vCenter Server kompatibel ist. Wählen Sie den 64-Bit-DSN aus, wenn Sie vom Installationsprogramm für vCenter Server zur Eingabe eines DSN aufgefordert werden.

Überprüfen, dass vCenter Server mit der lokalen Datenbank kommunizieren kann

Wenn sich Ihre Datenbank auf der gleichen Maschine befindet, auf der vCenter Server installiert werden soll und Sie den Namen dieser Maschine geändert haben, überprüfen Sie die Konfiguration. Stellen Sie sicher, dass der vCenter Server-DSN für die Kommunikation mit dem neuen Namen der Maschine konfiguriert ist.

Das Ändern des vCenter Server-Computernamens wirkt sich auf die Datenbankkommunikation aus, wenn sich der Datenbankserver auf demselben Computer wie der vCenter Server befindet. Falls Sie den Namen des Computers geändert haben, können Sie sicherstellen, dass die Kommunikation intakt bleibt.

Im Fall einer Remotedatenbank können Sie dieses Verfahren überspringen. Die Namensänderung wirkt sich nicht auf die Kommunikation mit Remotedatenbanken aus.

Überprüfen Sie nach dem Umbenennen des Servers zusammen mit dem Datenbankadministrator oder dem Datenbankanbieter, ob alle Komponenten der Datenbank funktionieren.

Voraussetzungen

- Stellen Sie sicher, dass der Datenbankserver läuft.
- Stellen Sie sicher, dass im DNS der vCenter Server-Computername aktualisiert wurde.

Vorgehensweise

1 Aktualisieren Sie ggf. die Datenquelleninformationen.

2 Pingen Sie den Namen des Computers an, um diese Verbindung zu testen.

Lautet der Computername beispielsweise `host-1.company.com`, führen Sie den folgenden Befehl an der Windows-Befehlszeile aus:

```
ping host-1.company.com
```

Ist der Ping-Test mit dem Computernamen erfolgreich, wurde der Name im DNS aktualisiert.

Die vCenter Server-Kommunikation ist bestätigt. Sie können mit der Vorbereitung anderer Komponenten in der Umgebung fortfahren.

Warten einer vCenter Server-Datenbank

Nachdem Sie die vCenter Server-Datenbankinstanz und vCenter Server installiert haben und diese funktionsfähig sind, führen Sie Standardprozesse zur Datenbankwartung durch.

Die Standardprozesse zur Datenbankwartung enthalten Folgendes:

- Überwachen der Protokolldateigröße und ggf. Komprimieren der Datenbankprotokolldatei.
- Planen regelmäßiger Sicherungen der Datenbank.
- Sichern der Datenbank vor einem vCenter Server-Upgrade.

Informationen zu spezifischen Wartungsvorgängen und zur Unterstützung finden Sie in der Dokumentation Ihres Datenbankanbieters.

Konfigurieren von Microsoft SQL Server-Datenbanken

Wenn Sie eine Microsoft SQL-Datenbank als Ihr vCenter Server-Repository verwenden möchten, konfigurieren Sie Ihre Datenbank für die Arbeit mit vCenter Server.

Vorgehensweise

1. Erstellen einer SQL Server-Datenbank und eines Benutzers für vCenter Server auf Seite 209

   Sie müssen eine Datenbank und einen Benutzer für vCenter Server erstellen. Sie können ein Skript zur Vereinfachung des Prozesses verwenden.

2. Festlegen von Datenbankberechtigungen durch das manuelle Erstellen von Datenbankrollen und des VMW-Schemas auf Seite 210

   Durch die Verwendung dieser mit vCenter Server 5.x und höher verfügbaren Methode kann der vCenter Server-Datenbankadministrator Berechtigungen für vCenter Server-Benutzer und -Administratoren festlegen, die über Microsoft SQL Server-Datenbankrollen erteilt werden können.

3. Festlegen von Datenbankberechtigungen durch die Verwendung des dbo-Schemas und der Datenbankrolle „db_owner“ auf Seite 211

   Bei Verwendung einer Microsoft SQL Server-Datenbank besteht die einfachste Methode zur Zuweisung von Berechtigungen zu einem vCenter Server-Datenbankbenutzer in der Datenbankrolle „db_owner“. Weisen Sie dem vCenter Server-Datenbankbenutzer die Rolle „db_owner“ sowohl in der vCenter Server- als auch in der MSDB-Datenbank zu.

4. Verwenden eines Skripts zum Erstellen eines vCenter Server-Benutzers mithilfe des Schemas „dbo“ und der Datenbankrolle „db_owner“ auf Seite 211

   Wenn Sie die Datenbankberechtigungen mit dem Schema „dbo“ und der Datenbankrolle „db_owner“ festlegen, können Sie ein Skript zum Erstellen eines vCenter Server-Benutzers mit der Datenbankrolle „db_owner“ verwenden.

5. Verwenden eines Skripts zum Erstellen und Anwenden von Microsoft SQL Server-Datenbankschemas und Rollen auf Seite 212

   Bei dieser Methode der Konfiguration der SQL-Datenbank können Sie das benutzerdefinierte VMW-Schema anstelle des vorhandenen dbo-Schemas verwenden. Darüber hinaus müssen Sie Datenbanküberwachung für einen Benutzer aktivieren, bevor Sie vCenter Server mit einem eingebetteten oder externen Platform Services Controller installieren.

6. (Optional) Verwenden eines Skripts zum manuellen Erstellen von Microsoft SQL Server-Datenbankobjekten auf Seite 214

   Mit dieser Konfigurationsmethode für die SQL-Datenbank können Sie Datenbankobjekte manuell erstellen.

7 Konfigurieren einer SQL Server-ODBC-Verbindung auf Seite 216

   Stellen Sie nach dem Erstellen eines vCenter Server-Benutzers eine Verbindung mit einer SQL Server-Datenbank her. Diese Verbindung ist für das Installieren einer vCenter Server-Instanz erforderlich.

8 Konfigurieren von Microsoft SQL Server TCP/IP für JDBC auf Seite 218

   Wenn TCP/IP von der Microsoft SQL Server-Datenbank deaktiviert ist und die dynamischen Ports nicht festgelegt sind, bleibt die JDBC-Verbindung geschlossen. Die geschlossen Verbindung sorgt dafür, dass die vCenter Server-Statistiken nicht korrekt funktionieren. Sie können das Server-TCP/IP für JDBC konfigurieren.

Erstellen einer SQL Server-Datenbank und eines Benutzers für vCenter Server

Sie müssen eine Datenbank und einen Benutzer für vCenter Server erstellen. Sie können ein Skript zur Vereinfachung des Prozesses verwenden.

Im Skript können Sie die Speicherorte der Daten und der Protokolldateien anpassen.

Der von diesem Skript erstellte Benutzer unterliegt keiner Sicherheitsrichtlinie. Ändern Sie die Kennwörter entsprechend.

Vorgehensweise

1 Melden Sie sich bei einer Microsoft SQL Server Management Studio-Sitzung als Sysadmin (SA) oder bei einem Benutzerkonto mit **Sysadmin**-Rechten an.

2 Führen Sie das folgende Skript aus.

   Das Skript befindet sich im vCenter Server-Installationspaket unter `/<Installationsverzeichnis>/vCenter-Server/dbschema/DB_and_schema_creation_scripts_MSSQL.txt`.

```
use [master]
go
CREATE DATABASE [VCDB] ON PRIMARY
(NAME = N'vcdb', FILENAME = N'C:\db\VCDB.mdf', SIZE = 10MB, FILEGROWTH = 10% )
LOG ON
(NAME = N'vcdb_log', FILENAME = N'C:\db\VCDB.ldf', SIZE = 1000KB, FILEGROWTH = 10%)
COLLATE SQL_Latin1_General_CP1_CI_AS
go
use VCDB
go
CREATE LOGIN [vpxuser] WITH PASSWORD=N'vpxuser!0', DEFAULT_DATABASE=VCDB, DEFAULT_LANGUA-
GE=us_english, CHECK_POLICY=OFF
go
CREATE USER [vpxuser] for LOGIN [vpxuser]
go
use MSDB
go
CREATE USER [vpxuser] for LOGIN [vpxuser]
go
```

Sie verfügen jetzt über eine Microsoft SQL Server-Datenbank, die Sie mit vCenter Server verwenden können.

Weiter

Weitere Informationen hierzu finden Sie unter „Festlegen von Datenbankberechtigungen durch das manuelle Erstellen von Datenbankrollen und des VMW-Schemas“, auf Seite 210.

Festlegen von Datenbankberechtigungen durch das manuelle Erstellen von Datenbankrollen und des VMW-Schemas

Durch die Verwendung dieser mit vCenter Server 5.x und höher verfügbaren Methode kann der vCenter Server-Datenbankadministrator Berechtigungen für vCenter Server-Benutzer und -Administratoren festlegen, die über Microsoft SQL Server-Datenbankrollen erteilt werden können.

Verwenden Sie diese Methode, da vCenter Server-Benutzer das dbo-Datenbankschema und die db_owner-Rolle für die Installation und das Upgrade von vCenter Server nicht mehr einrichten müssen.

Alternativ dazu können Sie vCenter Server-Datenbankberechtigungen zuweisen, indem Sie die db_owner-Rolle erstellen und zuweisen und vom vCenter Server-Installationsprogramm das Standardschema erstellen lassen, das dieser Rolle die Berechtigungen für Datenbankbenutzer zuweist. Siehe „Festlegen von Datenbankberechtigungen durch die Verwendung des dbo-Schemas und der Datenbankrolle „db_owner"", auf Seite 211.

Voraussetzungen

Erstellen Sie die vCenter Server-Datenbank. Siehe „Erstellen einer SQL Server-Datenbank und eines Benutzers für vCenter Server", auf Seite 209.

Vorgehensweise

1. Erstellen Sie die VCDB-Datenbank und das VMW-Datenbankschema in VCDB.
2. Weisen Sie dem Benutzer [vpxuser] das Standard-VMW-Schema zu.
3. Erstellen Sie in der vCenter Server-Datenbank die VC_ADMIN_ROLE-Benutzerrolle.
4. Weisen Sie in der vCenter Server-Datenbank der VC_ADMIN_ROLE-Rolle Berechtigungen zu.
   a. Erteilen Sie die Schemaberechtigungen ALTER, REFERENCES und INSERT.
   b. Erteilen Sie die Berechtigungen CREATE TABLE, VIEW und CREATE PROCEDURES.
5. Erstellen Sie in der vCenter Server-Datenbank die VC_USER_ROLE-Rolle.
6. Erteilen Sie in der vCenter Server-Datenbank die Schemaberechtigungen SELECT, INSERT, DELETE, UPDATE und EXECUTE für die VC_USER_ROLE-Rolle.
7. Erteilen Sie dem Benutzer [vpxuser] die VC_USER_ROLE-Rolle.
8. Erteilen Sie dem Benutzer [vpxuser] die VC_ADMIN_ROLE-Rolle.
9. Erstellen Sie in der MSDB-Datenbank den Benutzer [vpxuser].
10. Erstellen Sie in der MSDB-Datenbank die VC_ADMIN_ROLE-Rolle.
11. Erteilen Sie Berechtigungen für die VC_ADMIN_ROLE-Rolle in MSDB.
    a. Erteilen Sie in den MSDB-Tabellen „syscategories", „sysjobsteps", „sysjobs_view" und „sysjobs" dem Benutzer [vpxuser] die Berechtigung SELECT.
    b. Erteilen Sie in den gespeicherten MSDB-Prozeduren sp_add_job, sp_delete_job, sp_add_jobstep, sp_update_job, sp_add_jobserver, sp_add_jobschedule und sp_add_category der VC_ADMIN_ROLE-Rolle die Berechtigung EXECUTE.
12. Erteilen Sie in der MSDB-Datenbank dem Benutzer [vpxuser] die VC_ADMIN_ROLE-Rolle.
13. Erteilen Sie dem Benutzer [vpxuser] die Berechtigungen VIEW SERVER STATE und VIEW ANY DEFINITIONS.
14. Stellen Sie eine Verbindung zur vCenter Server-Datenbank als Benutzer [vpxuser] her und erstellen Sie den ODBC-DSN.
15. vCenter Server installieren.

16 Entziehen Sie in der MSDB-Datenbank dem Benutzer [vpxuser] die VC_ADMIN_ROLE-Rolle.

   Nachdem Sie die Rolle entzogen haben, können Sie sie inaktiv lassen, damit sie bei künftigen Upgrades verwendet werden kann, oder sie zwecks erhöhter Sicherheit entfernen. Falls Sie die Rolle entfernen, müssen Sie sie neu erstellen und dem Benutzer [vpxuser] zuweisen, bevor ein Upgrade von vCenter Server durchgeführt werden kann.

Die hartcodierte dbo-Rolle wird aus `VCDB_mssql.sql` entfernt.

Weiter

„Verwenden eines Skripts zum Erstellen und Anwenden von Microsoft SQL Server-Datenbankschemas und Rollen“, auf Seite 212

Festlegen von Datenbankberechtigungen durch die Verwendung des dbo-Schemas und der Datenbankrolle „db_owner“

Bei Verwendung einer Microsoft SQL Server-Datenbank besteht die einfachste Methode zur Zuweisung von Berechtigungen zu einem vCenter Server-Datenbankbenutzer in der Datenbankrolle „db_owner“. Weisen Sie dem vCenter Server-Datenbankbenutzer die Rolle „db_owner“ sowohl in der vCenter Server- als auch in der MSDB-Datenbank zu.

Alternativ können erfahrene Datenbankadministratoren die Berechtigungen festlegen, indem sie Datenbankrollen und das VMW-Datenbankschema manuell erstellen. Siehe „Festlegen von Datenbankberechtigungen durch das manuelle Erstellen von Datenbankrollen und des VMW-Schemas“, auf Seite 210 und „Verwenden eines Skripts zum Erstellen und Anwenden von Microsoft SQL Server-Datenbankschemas und Rollen“, auf Seite 212. Diese Methode, die ab vSphere 5.0 zur Verfügung steht, wird empfohlen, da sie dem Datenbankadministrator mehr Kontrolle über die Datenbankberechtigungen ermöglicht. Bei der empfohlenen Methode entfällt auch die Notwendigkeit der Einrichtung des Datenbankschemas „dbo“ und der Rolle „db_owner“ für vCenter Server-Benutzer, die vCenter Server installieren und aktualisieren.

Voraussetzungen

Erstellen Sie die vCenter Server-Datenbank. Siehe „Erstellen einer SQL Server-Datenbank und eines Benutzers für vCenter Server“, auf Seite 209.

Vorgehensweise

1 Weisen Sie „dbo“ der vCenter Server- und Microsoft SQL-Datenbank zu.

2 Weisen Sie allen Benutzern, die vCenter Server installieren oder aktualisieren möchten, das Standardschema „dbo“ zu.

Bei der Installation von vCenter Server verwendet das Installationsprogramm das Standardschema „dbo“, um der Rolle „db_owner“ Berechtigungen zuzuweisen.

Verwenden eines Skripts zum Erstellen eines vCenter Server -Benutzers mithilfe des Schemas „dbo“ und der Datenbankrolle „db_owner“

Wenn Sie die Datenbankberechtigungen mit dem Schema „dbo“ und der Datenbankrolle „db_owner“ festlegen, können Sie ein Skript zum Erstellen eines vCenter Server-Benutzers mit der Datenbankrolle „db_owner“ verwenden.

Alternativ können erfahrene Datenbankadministratoren die Berechtigungen festlegen, indem sie Datenbankrollen und die VMW- und SQL Server-Datenbankschemas erstellen. Siehe „Festlegen von Datenbankberechtigungen durch das manuelle Erstellen von Datenbankrollen und des VMW-Schemas“, auf Seite 210„Verwenden eines Skripts zum Erstellen und Anwenden von Microsoft SQL Server-Datenbank-

schemas und Rollen“, auf Seite 212. Diese Methode, die ab vSphere 5.0 zur Verfügung steht, wird empfohlen, da sie dem Datenbankadministrator mehr Kontrolle über die Datenbankberechtigungen ermöglicht. Bei dieser Methode entfällt die Notwendigkeit der Einrichtung der Datenbankrolle „dbo“ und des Schemas „db_owner“ für vCenter Server-Benutzer, die vCenter Server installieren und aktualisieren.

Voraussetzungen

Erstellen Sie die vCenter Server-Datenbank. Siehe „Erstellen einer SQL Server-Datenbank und eines Benutzers für vCenter Server“, auf Seite 209.

Vorgehensweise

1 Melden Sie sich bei Microsoft SQL Server Management Studio als Sysadmin oder mit einem Benutzerkonto mit **Sysadmin**-Rechten an.

2 Führen Sie das Skript aus, um den vCenter Server-Benutzer zu erstellen.

   Das Skript befindet sich in der Datei vCenter Server-Installationspaket/`*Installationsverzeichnis*/vCenter-Server/dbschema/DB_and_schema_creation_scripts_MSSQL.txt`.

```
use VCDB
go
sp_addrolemember @rolename = 'db_owner', @membername = 'vpxuser'
go
use MSDB
go
sp_addrolemember @rolename = 'db_owner', @membername = 'vpxuser'
go
```

Weiter

„Konfigurieren einer SQL Server-ODBC-Verbindung“, auf Seite 216

Verwenden eines Skripts zum Erstellen und Anwenden von Microsoft SQL Server-Datenbankschemas und Rollen

Bei dieser Methode der Konfiguration der SQL-Datenbank können Sie das benutzerdefinierte VMW-Schema anstelle des vorhandenen dbo-Schemas verwenden. Darüber hinaus müssen Sie Datenbanküberwachung für einen Benutzer aktivieren, bevor Sie vCenter Server mit einem eingebetteten oder externen Platform Services Controller installieren.

Bei dieser Methode müssen Sie neue Datenbankrollen erstellen und diese dem *Benutzer* der Datenbank zuweisen.

Siehe „Festlegen von Datenbankberechtigungen durch das manuelle Erstellen von Datenbankrollen und des VMW-Schemas“, auf Seite 210 und „Verwenden eines Skripts zum Erstellen und Anwenden von Microsoft SQL Server-Datenbankschemas und Rollen“, auf Seite 212.

Voraussetzungen

Erstellen Sie eine SQL Server-Datenbank und einen Benutzer für vCenter Server. Sie können die Datenbank manuell oder mithilfe eines Skripts erstellen. Siehe „Erstellen einer SQL Server-Datenbank und eines Benutzers für vCenter Server“, auf Seite 209.

Vorgehensweise

1 Melden Sie sich bei einer Microsoft SQL Server Management Studio-Sitzung als Sysadmin oder mit einem Benutzerkonto mit Sysadmin-Rechten an.

2 Führen Sie das folgende Skript zum Erstellen des Datenbankschemas und der Rollen aus.

   Das Skript im vCenter Server-Installationspaket befindet sich in der Datei `/`*`Installationsverzeichnis`*`/vCenter-Server/dbschema/DB_and_schema_creation_scripts_MSSQL.txt`.

```
CREATE SCHEMA [VMW]
go
ALTER USER [vpxuser] WITH DEFAULT_SCHEMA =[VMW]

if not exists (SELECT name FROM sysusers WHERE issqlrole=1 AND name = 'VC_ADMIN_ROLE')
CREATE ROLE VC_ADMIN_ROLE;
GRANT ALTER ON SCHEMA :: [VMW] to VC_ADMIN_ROLE;
GRANT REFERENCES ON SCHEMA :: [VMW] to VC_ADMIN_ROLE;
GRANT INSERT ON SCHEMA ::  [VMW] to VC_ADMIN_ROLE;

GRANT CREATE TABLE to VC_ADMIN_ROLE;
GRANT CREATE VIEW to VC_ADMIN_ROLE;
GRANT CREATE Procedure to VC_ADMIN_ROLE;

if not exists (SELECT name FROM sysusers WHERE issqlrole=1 AND name = 'VC_USER_ROLE')
CREATE ROLE VC_USER_ROLE
go
GRANT SELECT ON SCHEMA ::  [VMW] to VC_USER_ROLE
go
GRANT INSERT ON SCHEMA ::  [VMW] to VC_USER_ROLE
go
GRANT DELETE ON SCHEMA ::  [VMW] to VC_USER_ROLE
go
GRANT UPDATE ON SCHEMA ::  [VMW] to VC_USER_ROLE
go
GRANT EXECUTE ON SCHEMA :: [VMW] to VC_USER_ROLE
go
sp_addrolemember VC_USER_ROLE , [vpxuser]
go
sp_addrolemember VC_ADMIN_ROLE , [vpxuser]
go
use MSDB
go
if not exists (SELECT name FROM sysusers WHERE issqlrole=1 AND name = 'VC_ADMIN_ROLE')
CREATE ROLE VC_ADMIN_ROLE;
go
GRANT SELECT on msdb.dbo.syscategories to VC_ADMIN_ROLE
go
GRANT SELECT on msdb.dbo.sysjobsteps to VC_ADMIN_ROLE
go
GRANT SELECT ON msdb.dbo.sysjobs to VC_ADMIN_ROLE
go
GRANT SELECT ON msdb.dbo.sysjobs_view to VC_ADMIN_ROLE
go
GRANT EXECUTE ON msdb.dbo.sp_add_job TO VC_ADMIN_ROLE
go
GRANT EXECUTE ON msdb.dbo.sp_delete_job TO VC_ADMIN_ROLE
go
GRANT EXECUTE ON msdb.dbo.sp_add_jobstep TO VC_ADMIN_ROLE
go
GRANT EXECUTE ON msdb.dbo.sp_update_job TO VC_ADMIN_ROLE
```

```
go
GRANT EXECUTE ON msdb.dbo.sp_add_jobserver TO VC_ADMIN_ROLE
go
GRANT EXECUTE ON msdb.dbo.sp_add_jobschedule TO VC_ADMIN_ROLE
go
GRANT EXECUTE ON msdb.dbo.sp_add_category TO VC_ADMIN_ROLE
go
sp_addrolemember VC_ADMIN_ROLE , [vpxuser]
go
use master
go
grant VIEW SERVER STATE to [vpxuser]
go
GRANT VIEW ANY DEFINITION TO [vpxuser]
go
```

(Optional) Verwenden eines Skripts zum manuellen Erstellen von Microsoft SQL Server-Datenbankobjekten

Mit dieser Konfigurationsmethode für die SQL-Datenbank können Sie Datenbankobjekte manuell erstellen.

Alternativ dazu können Sie eine SQL-Server-ODBC-Verbindung konfigurieren und das Installationspaket ausführen. Das vCenter Server-Installationsprogramm erstellt Datenbankobjekte. Siehe „Konfigurieren einer SQL Server-ODBC-Verbindung“, auf Seite 216.

Bei der Verwendung eines Skripts zum manuellen Erstellen von Datenbankobjekten müssen Sie eine der folgenden Aktionen durchführen.

- Weisen Sie die db_owner-Rolle dem *Benutzer* der Datenbank in VCDB und in MSDB zu. Siehe „Festlegen von Datenbankberechtigungen durch die Verwendung des dbo-Schemas und der Datenbankrolle „db_owner““, auf Seite 211 und „Verwenden eines Skripts zum Erstellen eines vCenter Server-Benutzers mithilfe des Schemas „dbo“ und der Datenbankrolle „db_owner““, auf Seite 211.
- Weisen Sie die Rolle VC_ADMIN_ROLE dem *Benutzer* der Datenbank in VCDB und in MSDB zu und weisen Sie die Rolle VC_USER_ROLE dem *Benutzer* der Datenbank in VCDB zu. Siehe „Festlegen von Datenbankberechtigungen durch das manuelle Erstellen von Datenbankrollen und des VMW-Schemas“, auf Seite 210.

Voraussetzungen

Erstellen Sie die SQL Server-Datenbank. Sie können die SQL Server-Datenbank manuell oder mithilfe eines Skripts erstellen. Siehe „Erstellen einer SQL Server-Datenbank und eines Benutzers für vCenter Server“, auf Seite 209.

Vorgehensweise

1. Melden Sie sich bei der Microsoft SQL Server Management Studio-Sitzung als *Benutzername* für ein Benutzerkonto an, das Sie in den vCenter Server- und MSDB-Datenbanken erstellt haben.
2. Suchen Sie die „dbschema“-Skripts im Verzeichnis für vCenter Server-Installationspakete `/`*`Installationsverzeichnis`*`/vCenter-Server/dbschema`.
3. Öffnen Sie die Dateien `VCDB_mssql.SQL` und `Topn_DB_mssql.sql` mithilfe von Microsoft SQL Server Management Studio und ersetzen Sie alle Vorkommen von `$schema` durch den Schemanamen.
4. Öffnen Sie die Datei `VCDB_views_mssql.sql` mithilfe von Microsoft SQL Server Management Studio und ersetzen Sie alle Vorkommen von `;` durch `;` neue Zeile und `go`.

5 Führen Sie die Skripts in der richtigen Reihenfolge auf der Datenbank aus.

Der DBO-Benutzer muss die von diesen Skripts erstellten Objekte besitzen. Öffnen Sie in Microsoft SQL Server Management Studio ein Skript nach dem anderen und drücken Sie F5, um die Skripts in der hier angegebenen Reihenfolge auszuführen.

```
VCDB_mssql.SQL
insert_stats_proc_mssql.sql
load_stats_proc_mssql.sql
purge_stat2_proc_mssql.sql
purge_stat3_proc_mssql.sql
purge_usage_stats_proc_mssql.sql
stats_rollup1_proc_mssql.sql
stats_rollup2_proc_mssql.sql
stats_rollup3_proc_mssql.sql
cleanup_events_mssql.sql
delete_stats_proc_mssql.sql
upsert_last_event_proc_mssql.sql
load_usage_stats_proc_mssql.sql
TopN_DB_mssql.sql
calc_topn1_proc_mssql.sql
calc_topn2_proc_mssql.sql
calc_topn3_proc_mssql.sql
calc_topn4_proc_mssql.sql
clear_topn1_proc_mssql.sql
clear_topn2_proc_mssql.sql
clear_topn3_proc_mssql.sql
clear_topn4_proc_mssql.sql
rule_topn1_proc_mssql.sql
rule_topn2_proc_mssql.sql
rule_topn3_proc_mssql.sql
rule_topn4_proc_mssql.sql
process_license_snapshot_mssql.sql
l_stats_rollup3_proc_mssql.sql
l_purge_stat2_proc_mssql.sql
l_purge_stat3_proc_mssql.sql
l_stats_rollup1_proc_mssql.sql
l_stats_rollup2_proc_mssql.sql
VCDB_views_mssql.sql
```

6 (Optional) Sie können zudem die folgenden Skripts zum Aktiveren der Datenbank-Statusüberwachung ausführen.

```
job_dbm_performance_data_mssql.sql
process_performance_data_mssql.sql
```

7 Führen Sie für alle unterstützten Versionen von Microsoft SQL Server (außer Microsoft SQL Server Express) diese Skripts aus, um geplante Aufgaben für die Datenbank einzurichten.

Diese Skripts stellen sicher, dass der SQL Server Agent-Dienst ausgeführt wird.

```
job_schedule1_mssql.sql
job_schedule2_mssql.sql
job_schedule3_mssql.sql
job_cleanup_events_mssql.sql
job_topn_past_day_mssql.sql
job_topn_past_week_mssql.sql
job_topn_past_month_mssql.sql
job_topn_past_year_mssql.sql
```

8 Erteilen Sie für alle in Schritt 5 erstellten Prozeduren eine Ausführungsberechtigung für die vCenter Server-Datenbank.

```
grant execute on insert_stats_proc to vCenter_db_user
grant execute on purge_stat2_proc to vCenter_db_user
grant execute on purge_stat3_proc to vCenter_db_user
grant execute on purge_usage_stat_proc to vCenter_db_user
grant execute on stats_rollup1_proc to vCenter_db_user
grant execute on stats_rollup2_proc to vCenter_db_user
grant execute on stats_rollup3_proc to vCenter_db_user
grant execute on cleanup_events_tasks_proc to vCenter_db_user
grant execute on delete_stats_proc to vCenter_db_user
grant execute on upsert_last_event_proc to vCenter_db_user
grant execute on load_usage_stats_proc to vCenter_db_user
grant execute on load_stats_proc to vCenter_db_user
grant execute on calc_topn1_proc to vCenter_db_user
grant execute on calc_topn2_proc to vCenter_db_user
grant execute on calc_topn3_proc to vCenter_db_user
grant execute on calc_topn4_proc to vCenter_db_user
grant execute on clear_topn1_proc to vCenter_db_user
grant execute on clear_topn2_proc to vCenter_db_user
grant execute on clear_topn3_proc to vCenter_db_user
grant execute on clear_topn4_proc to vCenter_db_user
grant execute on rule_topn1_proc to vCenter_db_user
grant execute on rule_topn2_proc to vCenter_db_user
grant execute on rule_topn3_proc to vCenter_db_user
grant execute on rule_topn4_proc to vCenter_db_user
grant execute on process_license_snapshot_proc to vCenter_db_user
grant execute on l_stats_rollup3_proc to vCenter_db_user
grant execute on l_purge_stat2_proc to vCenter_db_user
grant execute on l_purge_stat3_proc to vCenter_db_user
grant execute on l_stats_rollup1_proc to vCenter_db_user
grant execute on l_stats_rollup2_proc to vCenter_db_user
```

Wenn Sie das Skript `process_performance_data_mssql.sql` in Schritt 5 ausführen, erteilen Sie die folgende Ausführungsberechtigung für die vCenter Server-Datenbank.

```
grant execute on process_performance_data_proc to vCenter_db_user
```

9 Erstellen Sie auf der Maschine, auf der Sie vCenter Server installieren möchten, einen DSN, der auf den Datenbankserver mit dem Schema verweist.

10 Führen Sie das vCenter Server-Installationsprogramm aus.

11 Wenn eine Datenbankreinitialisierungs-Warnmeldung im vCenter Server-Installationsprogramm angezeigt wird, wählen Sie die Option **Nicht überschreiben, vorhandene Datenbank beibehalten** aus und fahren Sie mit der Installation fort.

   Diese Meldung wird angezeigt, wenn Sie eine Datenbank verwenden, die vCenter Server-Tabellen aus einer vorherigen Installation einsetzt. Diese Meldung wird nicht angezeigt, wenn die Datenbank bereinigt ist.

12 Geben Sie die Datenbank-Benutzeranmeldung ein, wenn Sie dazu aufgefordert werden.

Konfigurieren einer SQL Server-ODBC-Verbindung

Stellen Sie nach dem Erstellen eines vCenter Server-Benutzers eine Verbindung mit einer SQL Server-Datenbank her. Diese Verbindung ist für das Installieren einer vCenter Server-Instanz erforderlich.

Wenn Sie SQL Server für vCenter Server verwenden, darf die Master-Datenbank nicht verwendet werden.

Spezifische Anweisungen zur Konfiguration der SQL Server-ODBC-Verbindung finden Sie in Ihrer Microsoft SQL Server-ODBC-Dokumentation.



VORSICHT Wenn Sie eine benannte Instanz von Microsoft SQL Server 2008 Standard Edition mit vCenter Server verwenden, benennen Sie die Instanz nicht „MSSQLSERVER". Wenn Sie die Instanz so benennen, funktioniert die JDBC-Verbindung nicht und bestimmte Funktionen, wie z. B. Leistungsdiagramme, stehen nicht zur Verfügung.

Voraussetzungen

- Überprüfen Sie die in „Konfigurationshinweise für die vCenter Server-Datenbank", auf Seite 206 angegebenen erforderlichen Datenbankpatches.
- Erstellen Sie eine Datenbank mit SQL Server Management Studio auf dem SQL-Server. Siehe „Erstellen einer SQL Server-Datenbank und eines Benutzers für vCenter Server", auf Seite 209.
- Legen Sie die Datenbankberechtigungen mithilfe einer der folgenden Optionen fest:
  - Option 1 (empfohlen): Befolgen Sie die unter „Festlegen von Datenbankberechtigungen durch das manuelle Erstellen von Datenbankrollen und des VMW-Schemas", auf Seite 210 und „Verwenden eines Skripts zum Erstellen und Anwenden von Microsoft SQL Server-Datenbankschemas und Rollen", auf Seite 212 beschriebenen Schritte.
  - Option 2 (alternativ): Befolgen Sie die unter „Festlegen von Datenbankberechtigungen durch die Verwendung des dbo-Schemas und der Datenbankrolle „db_owner"", auf Seite 211 und „Verwenden eines Skripts zum Erstellen eines vCenter Server-Benutzers mithilfe des Schemas „dbo" und der Datenbankrolle „db_owner"", auf Seite 211 beschriebenen Schritte.
- Stellen Sie SQL Native Client, Version 10 oder 11, bereit.

Vorgehensweise

1. Wählen Sie auf dem vCenter Server-System **Start > Verwaltung > Datenquellen (ODBC)** aus.
2. Ändern Sie auf der Registerkarte **System-DSN** eine vorhandene SQL Server-ODBC-Verbindung oder erstellen Sie eine neue SQL Server-ODBC-Verbindung.
   - Wählen Sie zum Ändern einer bestehenden SQL Server-ODBC-Verbindung die Verbindung in der Liste mit den Systemdatenquellen aus und klicken Sie auf **Konfigurieren** .

     WICHTIG Der vorhandene DSN muss SQL Native Client, Version 10 oder 11, verwenden.
   - Klicken Sie zum Erstellen einer neuen SQL Server ODBC-Verbindung auf **Hinzufügen**, wählen Sie **SQL Native Client** aus und klicken Sie auf **Beenden**.
3. Geben Sie einen ODBC-Datenquellennamen (DSN) in das Textfeld **Name** ein.

   Z. B. „VMware vCenter Server".
4. (Optional) Geben Sie eine ODBC-DSN-Beschreibung in das Feld **Beschreibung** ein.
5. Wählen Sie den Servernamen in der Dropdown-Liste **Server** aus.

   Geben Sie den SQL Server-Hostnamen in das Textfeld ein, falls er nicht im Dropdown-Menü vorhanden ist.
6. Wählen Sie eine Authentifizierungsmethode aus.
   - **Windows-Authentifizierung integrieren**.

Darüber hinaus können Sie den Dienstprinzipalnamen (Service Principal Name, SPN) eingeben

---

WICHTIG Diese Option kann nicht verwendet werden, wenn der vCenter Server-Dienst unter dem integrierten Systemkonto von Microsoft Windows ausgeführt wird.

- **SQL Server-Authentifizierung**.

  Geben Sie Ihren Benutzernamen und Ihr Kennwort für die Anmeldung beim SQL Server ein.

7 Wählen Sie im Menü **Die Standarddatenbank ändern auf** die für das vCenter Server-System erstellte Datenbank aus.

8 Klicken Sie auf **Beenden**.

9 Testen Sie in den SQL Server 2008-Editionen die Datenquelle, indem Sie im Menü **ODBC Microsoft SQL Server Setup** die Option **Datenquelle testen** auswählen und anschließend auf **OK** klicken.

10 Vergewissern Sie sich, dass der SQL-Agent auf Ihrem Datenbankserver ausgeführt wird.

Konfigurieren von Microsoft SQL Server TCP/IP für JDBC

Wenn TCP/IP von der Microsoft SQL Server-Datenbank deaktiviert ist und die dynamischen Ports nicht festgelegt sind, bleibt die JDBC-Verbindung geschlossen. Die geschlossen Verbindung sorgt dafür, dass die vCenter Server-Statistiken nicht korrekt funktionieren. Sie können das Server-TCP/IP für JDBC konfigurieren.

Diese Aufgabe bezieht sich auf Microsoft SQL Server-Remotedatenbankserver. Sie können diese Aufgabe überspringen, wenn es sich um eine lokale Datenbank handelt.

Vorgehensweise

1 Wählen Sie **Start > Alle Programme > Microsoft SQL Server > Configuration Tool > SQL Server Configuration Manager**.

2 Wählen Sie **SQL Server-Netzwerkkonfiguration > Protokolle für *Instanzname***.

3 Aktivieren Sie TCP/IP.

4 Öffnen Sie die TCP/IP-Eigenschaften.

5 Wählen Sie auf der Registerkarte **Protokoll** folgende Optionen.

Aktiviert	**Ja**
Alle Überwachen	**Ja**
Erhalten	**30000**

6 Wählen Sie auf der Registerkarte **IP-Adressen** folgende Optionen.



Aktiv	**Ja**
Dynamische TCP-Ports	**0**

7 Starten Sie den SQL Server-Dienst über **SQL Server Configuration Manager > SQL Server Services** neu.

8 Starten Sie den SQL Server-Browserdienst über **SQL Server Configuration Manager > SQL Server Services** neu.

Weiter

Optional können Sie die Datenbanküberwachung für Microsoft SQL-Datenbankbenutzer aktivieren. Ansonsten installieren Sie vCenter Server.

Konfigurieren von Oracle-Datenbanken

Wenn Sie eine Oracle-Datenbank als Ihr vCenter Server-Repository verwenden möchten, konfigurieren Sie Ihre Datenbank für die Arbeit mit vCenter Server.

Vorgehensweise

1 Verwenden eines Skripts zum Erstellen einer lokalen oder Remote-Oracle-Datenbank auf Seite 219

Wenn Sie eine Oracle-Datenbank mit vCenter Server verwenden, muss die Datenbank über bestimmte Tabellenspeicherplätze und Rechte verfügen. Sie können ein Skript ausführen, um die Erstellung der Datenbank zu vereinfachen. Sie können die Datenbank auch manuell erstellen.

2 Konfigurieren eines Oracle-Datenbankbenutzers auf Seite 220

Wenn Sie bei der Installation von vCenter Server eine Oracle-Datenbank verwenden möchten, müssen Sie den Datenbankbenutzer konfigurieren.

3 (Optional) Konfigurieren eines Oracle-Datenbankbenutzers für das Aktivieren der Datenbanküberwachung auf Seite 221

vCenter Server Database Monitoring erfasst Leistungsindikatoren, die es Administratoren ermöglichen, den Status des Datenbankservers festzustellen. Durch das Aktivieren der Datenbanküberwachung kann der Administrator Ausfallzeiten im vCenter verhindern, die aufgrund nicht ausreichender Ressourcen für den Datenbankserver eintreten.

4 (Optional) Verwenden eines Skripts zum Erstellen des Oracle-Datenbankschemas auf Seite 222

Das vCenter Server-Installationsprogramm erstellt das Schema während der Installation. Erfahrene Datenbankadministratoren, die die Schemaerstellung aufgrund von Umgebungsbeschränkungen umfassender steuern müssen, können wahlweise ein Skript zum Erstellen Ihres Datenbankschemas verwenden.

5 Konfigurieren einer Oracle-Verbindung für lokalen Zugriff auf Seite 223

Konfigurieren Sie eine Verbindung für lokalen Zugriff, wenn Sie vCenter Server auf demselben System wie die Oracle-Datenbank installieren.

6 Konfigurieren einer Oracle-Datenbankverbindung für den Remotezugriff auf Seite 224

Damit ein vCenter Server-System remote auf die Oracle-Datenbank zugreifen kann, muss eine Oracle-Verbindung konfiguriert werden.

7 Lokales Verbinden mit einer Oracle-Datenbank auf Seite 224

Bevor ein vCenter Server-System eine lokale Verbindung mit einer Oracle-Datenbank herstellen kann, müssen Sie die Verbindung einrichten.

Verwenden eines Skripts zum Erstellen einer lokalen oder Remote-Oracle-Datenbank

Wenn Sie eine Oracle-Datenbank mit vCenter Server verwenden, muss die Datenbank über bestimmte Tabellenspeicherplätze und Rechte verfügen. Sie können ein Skript ausführen, um die Erstellung der Datenbank zu vereinfachen. Sie können die Datenbank auch manuell erstellen.

Im Skript können Sie die Speicherorte der Daten und der Protokolldateien anpassen. Der von diesem Skript erstellte Benutzer unterliegt keiner Sicherheitsrichtlinie. Die Kennwörter werden nur angegeben, um die Arbeit zu erleichtern. Ändern Sie die Kennwörter entsprechend.

Vorgehensweise

1 Melden Sie sich mit dem Systemkonto bei einer SQL*Plus-Sitzung an.

2 Führen Sie das folgende Skript aus.

   Das Skript im vCenter Server-Installationspaket befindet sich in der Datei /*Installationsverzeichnis*/vCenter-Server/dbschema/DB_and_schema_creation_scripts_oracle.txt.

```
CREATE SMALLFILE TABLESPACE "VPX" DATAFILE '/u01/app/oracle/oradata/vcdb/vpx01.dbf'
SIZE 1G AUTOEXTEND ON NEXT 10M MAXSIZE UNLIMITED LOGGING EXTENT MANAGEMENT LOCAL SEGMENT
SPACE MANAGEMENT AUTO;
```

   Ändern Sie bei einer Windows-Installation den Verzeichnispfad auf die Datei vpx01.dbf.

Sie verfügen jetzt über eine Oracle-Datenbank, die Sie mit vCenter Server verwenden können.

Weiter

Sie können ein Skript zum Erstellen des Datenbankschemas ausführen.

Konfigurieren eines Oracle-Datenbankbenutzers

Wenn Sie bei der Installation von vCenter Server eine Oracle-Datenbank verwenden möchten, müssen Sie den Datenbankbenutzer konfigurieren.

Sie können eine Oracle-Datenbank für vCenter Server entweder lokal auf derselben Microsoft Windows-Maschine wie vCenter Server oder remote auf einem über das Netzwerk verbundenen Linux-, Unix- oder Microsoft Windows-Host konfigurieren.

Voraussetzungen

Überprüfen Sie die Softwareanforderungen für vCenter Server mit Oracle.

Vorgehensweise

1 Melden Sie sich mit dem Systemkonto bei einer SQL*Plus-Sitzung an.

2 Führen Sie den folgenden SQL-Befehl aus, um einen vCenter Server-Datenbankbenutzer mit den richtigen Berechtigungen zu erstellen.

   Das Skript befindet sich in der Datei /*Installationsverzeichnis*/vCenter-Server/dbschema/DB_and_schema_creation_scripts_oracle.txt des Installationspakets von vCenter Server.

   Im vorliegenden Beispiel ist „VPXADMIN“ der Benutzername.

```
CREATE USER "VPXADMIN" PROFILE "DEFAULT" IDENTIFIED BY "oracle" DEFAULT TABLESPACE
"VPX" ACCOUNT UNLOCK;
grant connect to VPXADMIN;
grant resource to VPXADMIN;
grant create view to VPXADMIN;
grant create sequence to VPXADMIN;
grant create table to VPXADMIN;
grant create materialized view to VPXADMIN;
grant execute on dbms_lock to VPXADMIN;
grant execute on dbms_job to VPXADMIN;
grant select on dba_lock to VPXADMIN;
grant select on dba_tablespaces to VPXADMIN;
grant select on dba_temp_files to VPXADMIN;
grant select on dba_data_files to VPXADMIN;
grant select on v_$session to VPXADMIN;
grant unlimited tablespace to VPXADMIN;
```

Standardmäßig werden der Rolle RESOURCE die Rechte **CREATE PROCEDURE**, **CREATE TABLE** und **CREATE SEQUENCE** zugewiesen. Falls diese Rechte der Rolle RESOURCE nicht zugewiesen wurden, gewähren Sie sie dem vCenter Server-Datenbankbenutzer.

HINWEIS Anstatt unbegrenzten Tablespace zu gewähren, können Sie ein bestimmtes Tablespace-Kontingent festlegen. Das empfohlene Kontingent ist unbegrenzt mit einer Mindestmenge von 500 MB. Führen Sie zum Festlegen eines unbegrenzten Kontingents den folgenden Befehl aus.

```
alter user "VPXADMIN" quota unlimited on "VPX";
```

Wenn Sie ein begrenztes Kontingent festlegen, überwachen Sie den verbleibenden Tablespace, um den folgenden Fehler zu vermeiden.

```
ORA-01536: space quota exceeded for tablespace '<tablespace>'
```

---

3 (Optional) Nachdem Sie vCenter Server erfolgreich mit der Oracle-Datenbank installiert haben, können Sie die folgenden Rechte widerrufen.

```
revoke select on dba_tablespaces from VPXADMIN;
revoke select on dba_temp_files from VPXADMIN;
revoke select on dba_data_files from VPXADMIN;
```

Sie verfügen jetzt über einen Oracle-Datenbankbenutzer, auf den Sie im vCenter Server-Installationsprogramm verweisen können.

Weiter

Erstellen Sie die Oracle-Datenbank mit allen benötigten Tabellenspeicherplätzen und Rechten.

(Optional) Konfigurieren eines Oracle-Datenbankbenutzers für das Aktivieren der Datenbanküberwachung

vCenter Server Database Monitoring erfasst Leistungsindikatoren, die es Administratoren ermöglichen, den Status des Datenbankservers festzustellen. Durch das Aktivieren der Datenbanküberwachung kann der Administrator Ausfallzeiten im vCenter verhindern, die aufgrund nicht ausreichender Ressourcen für den Datenbankserver eintreten.

Datenbanküberwachung für vCenter Server ermöglicht es Administratoren, die CPU des Datenbankservers, den Arbeitsspeicher, die E/A, den Datenspeicher und andere Umgebungsfaktoren für Stresszustände zu überwachen. Die Statistiken werden in den vCenter Server-Profilprotokolldateien gespeichert.

Aktivieren Sie vor oder nach der Installation von vCenter Server die Datenbanküberwachung für einen Benutzer. Sie können diesen Vorgang durchführen, während vCenter Server ausgeführt wird.

Vorgehensweise

1 Melden Sie sich mit dem Systemkonto bei einer SQL*Plus-Sitzung an.

2 Führen Sie die folgenden SQL-Befehle aus, um dem vCenter Server-Datenbankbenutzer zusätzliche Berechtigungen zu gewähren:

```
grant select on v_$system_event to user;
grant select on v_$sysmetric_history to user;
grant select on v_$sysstat to user;
grant select on dba_data_files to user;
grant select on v_$loghist to user;
```

Die vCenter-Datenbanküberwachung wird aktiviert.

(Optional) Verwenden eines Skripts zum Erstellen des Oracle-Datenbankschemas

Das vCenter Server-Installationsprogramm erstellt das Schema während der Installation. Erfahrene Datenbankadministratoren, die die Schemaerstellung aufgrund von Umgebungsbeschränkungen umfassender steuern müssen, können wahlweise ein Skript zum Erstellen Ihres Datenbankschemas verwenden.

Informationen zum Erstellen eines Schemas mithilfe des vCenter Server-Installationsprogramms in Abhängigkeit der jeweiligen Umgebung finden Sie unter „Konfigurieren einer Oracle-Verbindung für lokalen Zugriff“, auf Seite 223 oder „Konfigurieren einer Oracle-Datenbankverbindung für den Remotezugriff“, auf Seite 224.

Voraussetzungen

Erstellen Sie die Oracle-Datenbank und den Benutzer. Sie können die Oracle-Datenbank und den Benutzer manuell oder mithilfe von Skripts erstellen.

Vorgehensweise

1 Öffnen Sie ein SQL*Plus-Fenster mit einem Benutzer, der über Schemabesitzerrechte für die vCenter Server-Datenbank verfügt.

2 Suchen Sie die „dbschema“-Skripts im Verzeichnis für vCenter Server-Installationspakete `/`*`Installationsverzeichnis`*`/vCenter-Server/dbschema`.

3 Führen Sie die Skripts in SQL*Plus in der richtigen Reihenfolge aus.

   `Pfad` ist der Verzeichnispfad zum Ordner `/`*`Installationsverzeichnis`*`/vCenter-Server/dbschema`.

```
@path/VCDB_oracle.SQL
@path/VCDB_views_oracle.SQL
@path/insert_stats_proc_oracle.sql
@path/load_stats_proc_oracle.sql
@path/purge_stat2_proc_oracle.sql
@path/purge_stat3_proc_oracle.sql
@path/purge_usage_stats_proc_oracle.sql
@path/stats_rollup1_proc_oracle.sql
@path/stats_rollup2_proc_oracle.sql
@path/stats_rollup3_proc_oracle.sql
@path/cleanup_events_oracle.sql
@path/delete_stats_proc_oracle.sql
@path/load_usage_stats_proc_oracle.sql
@path/TopN_DB_oracle.sql
@path/calc_topn1_proc_oracle.sql
@path/calc_topn2_proc_oracle.sql
@path/calc_topn3_proc_oracle.sql
@path/calc_topn4_proc_oracle.sql
@path/clear_topn1_proc_oracle.sql
@path/clear_topn2_proc_oracle.sql
@path/clear_topn3_proc_oracle.sql
@path/clear_topn4_proc_oracle.sql
@path/rule_topn1_proc_oracle.sql
@path/rule_topn2_proc_oracle.sql
@path/rule_topn3_proc_oracle.sql
@path/rule_topn4_proc_oracle.sql
@path/process_license_snapshot_oracle.sql
@path/l_purge_stat2_proc_oracle.sql
```

```
@path/l_purge_stat3_proc_oracle.sql
@path/l_stats_rollup1_proc_oracle.sql
@path/l_stats_rollup2_proc_oracle.sql
@path/l_stats_rollup3_proc_oracle.sql
```

4 (Optional) Sie können zudem die folgenden Skripts zum Aktiveren der Datenbank-Statusüberwachung ausführen.

```
job_dbm_performance_data_oracle.sql
process_performance_data_oracle.sql
```

5 Führen Sie für alle unterstützten Versionen von Oracle Server diese Skripts aus, um geplante Aufgaben für die Datenbank einzurichten.

```
@Pfad/job_schedule1_oracle.sql
@Pfad/job_schedule2_oracle.sql
@Pfad/job_schedule3_oracle.sql
@Pfad/job_cleanup_events_oracle.sql
@Pfad/job_topn_past_day_oracle.sql
@Pfad/job_topn_past_week_oracle.sql
@Pfad/job_topn_past_month_oracle.sql
@Pfad/job_topn_past_year_oracle.sql
```

Sie verfügen jetzt über ein mit vCenter Server kompatibles Datenbankschema.

6 Erstellen Sie auf der Maschine, auf der Sie vCenter Server installieren möchten, einen DSN, der auf den Datenbankserver mit dem Schema verweist.

7 Führen Sie das vCenter Server-Installationsprogramm aus.

8 Wenn eine Datenbankreinitialisierungs-Warnmeldung im vCenter Server-Installationsprogramm angezeigt wird, wählen Sie die Option **Nicht überschreiben, vorhandene Datenbank beibehalten** aus und fahren Sie mit der Installation fort.

   Diese Meldung wird angezeigt, wenn Sie eine Datenbank verwenden, die vCenter Server-Tabellen aus einer vorherigen Installation einsetzt. Diese Meldung wird nicht angezeigt, wenn die Datenbank bereinigt ist.

9 Geben Sie die Datenbank-Benutzeranmeldung ein, wenn Sie dazu aufgefordert werden.

Das Oracle-Datenbankschema wird erstellt.

Konfigurieren einer Oracle-Verbindung für lokalen Zugriff

Konfigurieren Sie eine Verbindung für lokalen Zugriff, wenn Sie vCenter Server auf demselben System wie die Oracle-Datenbank installieren.

Voraussetzungen

Überprüfen Sie die in „Konfigurationshinweise für die vCenter Server-Datenbank“, auf Seite 206 angegebenen erforderlichen Datenbankpatches. Wenn die Datenbank nicht ordnungsgemäß vorbereitet wurde, zeigt das Installationsprogramm von vCenter Server Fehler- und Warnmeldungen an.

Vorgehensweise

1 Laden Sie Oracle 11g oder Oracle 12c von der Oracle Website herunter.

2 Installieren Sie Oracle 11g oder Oracle 12c und erstellen Sie eine Datenbank.

3 Konfigurieren Sie die Option „TNS-Dienstname“ im ODBC-DSN.

   Der TNS-Dienstname ist der Netzdienstname für die Datenbank, mit der Sie eine Verbindung herstellen möchten. Sie finden den Netzdienstnamen in der Datei `tnsnames.ora` im Ordner `NETWORK\ADMIN` im Installationspfad der Oracle-Datenbank.

Die Datenbank ist für lokalen Zugriff konfiguriert.

Konfigurieren einer Oracle-Datenbankverbindung für den Remotezugriff

Damit ein vCenter Server-System remote auf die Oracle-Datenbank zugreifen kann, muss eine Oracle-Verbindung konfiguriert werden.

Voraussetzungen

Überprüfen Sie die in „Konfigurationshinweise für die vCenter Server-Datenbank“, auf Seite 206 angegebenen erforderlichen Datenbankpatches. Wenn die Datenbank nicht ordnungsgemäß vorbereitet wurde, zeigt das Installationsprogramm von vCenter Server Fehler- und Warnmeldungen an.

Vorgehensweise

1 Verwenden Sie einen Texteditor oder den Net8-Konfigurationsassistenten, um die Datei `tnsnames.ora` im Verzeichnis `C:\Oracle\Oraxx\NETWORK\ADMIN` zu bearbeiten, wobei `xx` entweder 10g oder 11g ist.

   Fügen Sie den folgenden Eintrag hinzu, wobei `HOST` für den verwalteten Host steht, mit dem der Client eine Verbindung herstellen muss.

```
VPX =
(DESCRIPTION =
(ADDRESS_LIST =
(ADDRESS=(PROTOCOL=TCP)(HOST=vpxd-Oracle)(PORT=1521))
   )
(CONNECT_DATA =
(SERVICE_NAME = VPX)
   )
   )
```

2 Konfigurieren Sie die Option „TNS-Dienstname“ im ODBC-DSN.

   Der TNS-Dienstname ist der Netzdienstname für die Datenbank, mit der Sie verbinden möchten, in diesem Fall „VPX“. Sie finden den Netzdienstnamen in der Datei `tnsnames.ora`.

Lokales Verbinden mit einer Oracle-Datenbank

Bevor ein vCenter Server-System eine lokale Verbindung mit einer Oracle-Datenbank herstellen kann, müssen Sie die Verbindung einrichten.

Vorgehensweise

◆ Stellen Sie eine ODBC-Verbindung zur Datenbank her.

   Der folgende Code stellt Beispieleinstellungen dar.

```
Data Source Name: VMware vCenter Server  TNS Service Name: VPX  User Id: vpxAdmin
```

Sie verfügen jetzt über eine Datenbank, mit der Sie lokal eine Verbindung herstellen können.

Weiter

Sie können die Datenbanküberwachung für Oracle-Datenbankbenutzer aktivieren. Ansonsten installieren Sie vCenter Server.

Datenbankberechtigungsanforderungen für vCenter Server

Für vCenter Server ist eine Datenbank erforderlich. Wenn Sie beim Erstellen der Datenbank eine externe Oracle- oder Microsoft SQL Server-Datenbank verwenden möchten, müssen Sie dem Datenbankbenutzer bestimmte Berechtigungen zuweisen.

Tabelle 7-2. Microsoft SQL-Datenbankberechtigungen für vCenter Server

Berechtigung	Beschreibung
GRANT ALTER ON SCHEMA :: [VMW] TO VC_ADMIN_ROLE	Obligatorisch beim Arbeiten mit einem benutzerdefinierten SQL Server-Schema.
GRANT REFERENCES ON SCHEMA :: [VMW] TO VC_ADMIN_ROLE	Obligatorisch beim Arbeiten mit einem benutzerdefinierten SQL Server-Schema.
GRANT INSERT ON SCHEMA :: [VMW] TO VC_ADMIN_ROLE	Obligatorisch beim Arbeiten mit einem benutzerdefinierten SQL Server-Schema.
GRANT CREATE TABLE TO VC_ADMIN_ROLE	Notwendig zum Erstellen einer Tabelle.
GRANT CREATE VIEW TO VC_ADMIN_ROLE	Notwendig zum Erstellen einer Ansicht.
GRANT CREATE PROCEDURE TO VC_ADMIN_ROLE	Notwendig zum Erstellen einer gespeicherten Prozedur.
GRANT SELECT ON SCHEMA :: [VMW] TO VC_USER_ROLE	Berechtigungen zum Ausführen von Auswahl-, Einfüg-, Lösch- und Aktualisierungsfunktionen (SELECT, INSERT, DELETE, UPDATE) bei Tabellen, die Teil des VMW-Schemas sind.
GRANT INSERT ON SCHEMA :: [VMW] TO VC_USER_ROLE	
GRANT DELETE ON SCHEMA :: [VMW] TO VC_USER_ROLE	
GRANT UPDATE ON SCHEMA :: [VMW] TO VC_USER_ROLE	
GRANT EXECUTE ON SCHEMA :: [VMW] TO VC_USER_ROLE	Notwendig zum Ausführen einer gespeicherten Prozedur im Datenbankschema.
GRANT SELECT ON msdb.dbo.syscategories TO VC_ADMIN_ROLE	Notwendig zum Bereitstellen von SQL Server-Aufträgen. Diese Berechtigungen sind nur bei der Installation und beim Upgrade, aber nicht mehr nach der Bereitstellung erforderlich.
GRANT SELECT ON msdb.dbo.sysjobsteps TOVC_ADMIN_ROLE	
GRANT SELECT ON msdb.dbo.sysjobs TO VC_ADMIN_ROLE	
GRANT EXECUTE ON msdb.dbo.sp_add_job TO VC_ADMIN_ROLE	
GRANT EXECUTE ON msdb.dbo.sp_delete_job TO VC_ADMIN_ROLE	
GRANT EXECUTE ON msdb.dbo.sp_add_jobstep TO VC_ADMIN_ROLE	
GRANT EXECUTE ON msdb.dbo.sp_update_job TO VC_ADMIN_ROLE	
GRANT EXECUTE ON msdb.dbo.sp_add_jobserver TO VC_ADMIN_ROLE	
GRANT EXECUTE ON msdb.dbo.sp_add_jobschedule TO VC_ADMIN_ROLE	
GRANT EXECUTE ON msdb.dbo.sp_add_category TO VC_ADMIN_ROLE	

Tabelle 7-2. Microsoft SQL-Datenbankberechtigungen für vCenter Server (Fortsetzung)

Berechtigung	Beschreibung
GRANT VIEW SERVER STATE TO [vpxuser]	Bietet Zugriff auf dynamische Verwaltungsansichten von SQL Server und ermöglicht die Ausführung von sp_lock.
GRANT VIEW ANY DEFINITION TO [vpxuser]	Erforderlich, um dem Benutzer die Berechtigungen zum Anzeigen von Metadaten für SQL Server-Objekte zuzuweisen.

Tabelle 7-3. Oracle-Datenbankberechtigungen für vCenter Server

Berechtigung	Beschreibung
GRANT CONNECT TO VPXADMIN	Erforderlich für eine Verbindung mit der Oracle-Datenbank.
GRANT RESOURCE TO VPXADMIN	Notwendig zum Erstellen eines Auslösers, einer Sequenz, eines Typs, einer Prozedur usw. Standardmäßig werden der Rolle RESOURCE die Rechte CREATE PROCEDURE, CREATE TABLE und CREATE SEQUENCE zugewiesen. Falls diese Rechte der Rolle RESOURCE nicht zugewiesen wurden, gewähren Sie sie dem vCenter Server-Datenbankbenutzer.
GRANT CREATE VIEW TO VPXADMIN	Notwendig zum Erstellen einer Ansicht.
GRANT CREATE SEQUENCE TO VPXADMIN	Notwendig zum Erstellen einer Sequenz.
GRANT CREATE TABLE TO VPXADMIN	Notwendig zum Erstellen einer Tabelle.
GRANT CREATE MATERIALIZED VIEW TO VPXADMIN	Notwendig zum Erstellen einer materialisierten Ansicht.
GRANT EXECUTE ON dbms_lock TO VPXADMIN	Notwendig zur Sicherstellung, dass die vCenter Server-Datenbank von einer einzelnen vCenter Server-Instanz verwendet wird.
GRANT EXECUTE ON dbms_job TO VPXADMIN	Notwendig bei Installation und Upgrade zum Planen und Verwalten der SQL-Aufträge. Diese Berechtigung ist nach der Bereitstellung nicht mehr erforderlich.
GRANT SELECT ON dba_lock TO VPXADMIN	Notwendig zum Ermitteln vorhandener Sperren auf der vCenter Server-Datenbank.
GRANT SELECT ON dba_tablespaces TO VPXADMIN	Notwendig beim Upgrade zum Ermitteln des erforderlichen Festplattenspeicherplatzes. Diese Berechtigung ist nach der Bereitstellung nicht mehr erforderlich.
GRANT SELECT ON dba_temp_files TO VPXADMIN	Notwendig beim Upgrade zum Ermitteln des erforderlichen Festplattenspeicherplatzes. Diese Berechtigung ist nach der Bereitstellung nicht mehr erforderlich.
GRANT SELECT ON dba_data_files TO VPXADMIN	Notwendig zum Überwachen des freien Speicherplatzes, während vCenter Server arbeitet.
GRANT SELECT ON v_$session TO VPXADMIN	Verwendete Ansicht zum Ermitteln vorhandener Sperren auf der vCenter Server-Datenbank.
GRANT UNLIMITED TABLESPACE TO VPXADMIN	Notwendig, um dem Benutzer der vCenter Server-Datenbank unbegrenzte Tablespace-Berechtigungen zuzuweisen.
GRANT SELECT ON v_$system_event TO VPXADMIN	Notwendig zum Prüfen der Protokolldateiwechsel.
GRANT SELECT ON v_$sysmetric_history TO VPXADMIN	Notwendig zum Prüfen der CPU-Nutzung.
GRANT SELECT ON v_$sysstat TO VPXADMIN	Notwendig zum Ermitteln der Puffercache-Zugriffsrate.

Tabelle 7-3. Oracle-Datenbankberechtigungen für vCenter Server (Fortsetzung)

Berechtigung	Beschreibung
GRANT SELECT ON dba_data_files TO VPXADMIN	Notwendig zum Ermitteln der Tablespace-Nutzung.
GRANT SELECT ON v_$loghist TO VPXADMIN	Notwendig zum Prüfen der Prüfpunkt-Häufigkeit.

Mit den Berechtigungen zur Master-Datenbank können Sie die vCenter Server-Datenbank überwachen, sodass zum Beispiel beim Erreichen eines bestimmten Grenzwerts eine Warnung angezeigt wird.

Auswirkungen von vCenter Single Sign On auf Installationen

vSphere beinhaltet ab Version 5.1 den vCenter Single Sign On-Dienst als Teil der vCenter Server-Managementinfrastruktur. Diese Änderung wirkt sich auf die vCenter Server-Installation aus.

Durch die Authentifizierung mit vCenter Single Sign On wird vSphere sicherer, da die vSphere-Softwarekomponenten miteinander über einen sicheren Token-Austauschmechanismus kommunizieren und sich alle anderen Benutzer ebenfalls mit vCenter Single Sign On authentifizieren.

Ab vSphere 6.0 ist vCenter Single Sign On entweder in einer eingebetteten Bereitstellung enthalten oder Bestandteil des Platform Services Controller. Der Platform Services Controller enthält alle Dienste, die für die Kommunikation zwischen vSphere-Komponenten erforderlich sind, darunter vCenter Single Sign On, VMware Certificate Authority, VMware Lookup Service und den Lizenzierungsdienst.

Die Installationsreihenfolge ist wichtig.

Erste Installation

Wenn Ihre Installation verteilt ist, müssen Sie den Platform Services Controller installieren, bevor Sie vCenter Server installieren oder die vCenter Server Appliance bereitstellen. Bei einer eingebetteten Bereitstellung wird die richtige Installationsreihenfolge automatisch eingehalten.

Nachfolgende Installationen

Für ca. bis zu acht vCenter Server-Instanzen kann ein Platform Services Controller die gesamte vSphere-Umgebung bedienen. Sie können die neuen vCenter Server-Instanzen mit dem gleichen Platform Services Controller verbinden. Für mehr als ca. acht vCenter Server-Instanzen können Sie einen zusätzlichen Platform Services Controller installieren, um die Leistung zu verbessern. Der vCenter Single Sign On-Dienst auf jedem Platform Services Controller synchronisiert Authentifizierungsdaten mit allen anderen Instanzen. Die genaue Zahl hängt neben anderen Faktoren davon ab, wie stark die vCenter Server-Instanzen genutzt werden.

Komponenten für vCenter Single Sign On

vCenter Single Sign On umfasst den Security Token Service (STS), einen Verwaltungsserver, einen vCenter Lookup Service und den VMware-Verzeichnisdienst (vmdir). Der VMware-Verzeichnisdienst wird auch für die Zertifikatverwaltung eingesetzt.

Während der Installation werden die Komponenten als Teil einer eingebetteten Implementierung oder als Teil des Platform Services Controller bereitgestellt.

STS (Security Token Service)

Der STS-Dienst gibt Security Assertion Markup Language-Token (SAML) aus. Diese Sicherheitstoken stellen die Identität eines Benutzers in einem der von vCenter Single Sign On unterstützten Identitätsquellentypen dar. Die SAML-Token ermöglichen Benutzern und Lösungsbenutzern, die sich erfolgreich bei vCenter Single Sign On authentifizieren, jeden von vCenter Single Sign On unterstützten vCenter-Dienst zu verwenden, ohne sich erneut bei jedem Dienst authentifizieren zu müssen.

Der vCenter Single Sign On-Dienst signiert alle Token mit einem Signierzertifikat und speichert das Tokensignierzertifikat auf der Festplatte. Das Zertifikat für den Dienst selbst wird ebenfalls auf der Festplatte gespeichert.

Verwaltungsserver

Mithilfe des Verwaltungsservers können Benutzer, die Administratorrechte für vCenter Single Sign On haben, den vCenter Single Sign On-Server konfigurieren und Benutzer und Gruppen auf dem vSphere Web Client verwalten. Anfänglich hat nur der Benutzer „administrator@*ihr_domänenname*" diese Berechtigungen. In vSphere 5.5 war dieser Benutzer „administrator@vsphere.local". In vSphere 6.0 können Sie die vSphere-Domäne ändern, wenn Sie vCenter Server installieren oder vCenter Server Appliance mit einem neuen Platform Services Controller bereitstellen. Benennen Sie die Domäne nicht mit Ihrem Microsoft Active Directory- oder OpenLDAP-Domänennamen.

VMware-Verzeichnisdienst (vmdir)

Der VMware-Verzeichnisdienst (vmdir) ist der Domäne zugeordnet, die Sie während der Installation angeben, und wird in jede eingebettete Bereitstellung sowie auf jedem Platform Services Controller eingeschlossen. Dieser Dienst ist ein mehrmandantenfähiger Multimaster-Verzeichnisdienst, der ein LDAP-Verzeichnis auf Port 389 zur Verfügung stellt. Der Dienst nutzt für Abwärtskompatibilität mit vSphere 5.5 und früheren Systemen nach wie vor Port 11711.

Wenn Ihre Umgebung mehr als eine Instanz des Platform Services Controller enthält, wird eine Aktualisierung des vmdir-Inhalts in einer vmdir-Instanz auf alle anderen Instanzen von vmdir propagiert.

Ab vSphere 6.0 speichert der VMware-Verzeichnisdienst nicht nur vCenter Single Sign On-Informationen, sondern auch Zertifikatsinformationen.

Identitäts-Verwaltungsdienst

Bearbeitete Identitätsquellen und STS-Authentifizierungsanforderungen.

Einrichten des vCenter Server -Administratorbenutzers

Die Art und Weise, wie der vCenter Server-Administratorbenutzer eingerichtet wird, hängt von der vCenter Single Sign On-Bereitstellung ab.

In vSphere-Versionen vor vSphere 5.1 sind vCenter Server-Administratoren diejenigen Benutzer, die zur lokalen Administratorgruppe des Betriebssystems gehören.

Wenn Sie in vSphere 5.1.x, 5.5 und 6.0 vCenter Server installieren, müssen Sie den standardmäßigen (anfänglichen) vCenter Server-Administratorbenutzer bzw. die standardmäßige Administratorgruppe angeben. Für Bereitstellungen, bei denen sich vCenter Server und vCenter Single Sign On auf der gleichen virtuellen Maschine bzw. dem gleichen physischen Server befinden, können Sie die lokale Betriebssystemgruppe „Administratoren" als administrative vCenter Server-Benutzer festlegen. Diese Option ist der Standard. Dieses Verhalten hat sich seit vCenter Server 5.0 nicht geändert.

Für größere Installationen, bei denen vCenter Single Sign On im Rahmen des Platform Services Controller und vCenter Server auf unterschiedlichen virtuellen Maschinen oder physischen Servern bereitgestellt werden, können Sie nicht so vorgehen wie in vCenter Server 5.0. Stattdessen müssen Sie die vCenter Server-Administratorrolle einem Benutzer oder einer Gruppe von einer Identitätsquelle zuweisen, die beim vCenter Single Sign On-Server registriert ist: Active Directory, OpenLDAP oder die Systemidentitätsquelle.

Authentifizieren für die vCenter Server -Umgebung

In vCenter Server 5.1 und höher authentifizieren sich Benutzer über vCenter Single Sign On.

Wenn in vCenter Server-Versionen vor vCenter Server 5.1 ein Benutzer eine Verbindung zu vCenter Server herstellt, authentifiziert vCenter Server den Benutzer, indem dieser anhand einer Active Directory-Domäne bzw. der Liste der lokalen Benutzer des Betriebssystems validiert wird.

Der Benutzer „administrator@*ihr_domänenname*" hat standardmäßig vCenter Single Sign-On-Administratorberechtigungen. Bei Anmeldung beim vCenter Single Sign On-Server über vSphere Web Client kann der Benutzer „administrator@*ihr_domänenname*" anderen Benutzern vCenter Single Sign On-Administratorrechte zuweisen. Diese Benutzer können sich von den Benutzern unterscheiden, die vCenter Server verwalten.

Die Benutzer können sich bei vCenter Server mit dem vSphere Web Client anmelden. Die Benutzer authentifizieren sich bei vCenter Single Sign On. Benutzer können alle vCenter Server-Instanzen anzeigen, für die der Benutzer über Berechtigungen verfügt. Nachdem die Benutzer eine Verbindung zu vCenter Server hergestellt haben, ist keine weitere Authentifizierung erforderlich. Welche Aktionen Benutzer für Objekte durchführen können, hängt von den vCenter Server-Berechtigungen des Benutzers für diese Objekte ab.

Weitere Informationen über vCenter Single Sign On finden Sie unter *vSphere-Sicherheit*.

Auswirkungen von vCenter Single Sign On auf das Anmeldeverhalten

Das Anmeldeverhalten von vCenter Single Sign On hängt von der Domäne, der der Benutzer angehört, und von den Identitätsquellen ab, die Sie vCenter Single Sign On hinzugefügt haben.

Wenn sich ein Benutzer vom vSphere Web Client aus bei einem vCenter Server-System anmeldet, hängt das Anmeldeverhalten davon ab, ob der Benutzer sich in der Standarddomäne befindet, d. h., in der als Standard-Identitätsquelle festgelegten Domäne.

- Benutzer, die sich in der Standarddomäne befinden, können sich mit ihrem Benutzernamen und Kennwort anmelden.
- Benutzer in einer Domäne, die vCenter Single Sign On als Identitätsquelle hinzugefügt wurde, aber nicht die Standarddomäne ist, können sich bei vCenter Server anmelden, müssen dazu aber die Domäne mit einer der folgenden Methoden angeben.
  - Mit Präfix des Domänennamens, beispielsweise MEINEDOMÄNE\Benutzer1
  - Mit der Domäne, beispielsweise benutzer1@meinedomäne.com
- Benutzer in einer Domäne, die keine Identitätsquelle von vCenter Single Sign On ist, können sich nicht bei vCenter Server anmelden. Wenn die Domäne, die Sie in vCenter Single Sign On hinzufügen, zu einer Domänenhierarchie gehört, bestimmt Active Directory, ob die Benutzer anderer Domänen der Hierarchie authentifiziert werden oder nicht.

Authentifizierungsberechtigungen, die das Resultat von geschachtelten Gruppen aus unterschiedlichen Identitätsquellen sind, werden von vCenter Single Sign On nicht weitergegeben. Wenn Sie beispielsweise die Gruppe der Domänenadministratoren zur Gruppe der lokalen Administratoren hinzufügen, werden die Berechtigungen nicht weitergegeben, da „Lokales Betriebssystem" und „Active Directory" separate Identitätsquellen sind.

Nach der Installation auf einem Windows-System verfügt der Benutzer „administrator@*ihr_domänenname*" über Administratorberechtigungen für den vCenter Single Sign On-Server und das vCenter Server-System.

Nach dem Bereitstellen der vCenter Server Appliance verfügt der Benutzer „administrator@*ihr_domänenname*" über Administratorberechtigungen für den vCenter Single Sign On-Server und das vCenter Server-System.

Identitätsquellen für vCenter Server mit vCenter Single Sign On

Sie können Identitätsquellen verwenden, um vCenter Single Sign On eine oder mehrere Domänen hinzuzufügen. Bei einer Domäne handelt es sich um ein Repository für Benutzer und Gruppen, das der vCenter Single Sign On-Server für die Benutzerauthentifizierung verwenden kann.

Eine Identitätsquelle ist eine Sammlung von Benutzer- und Gruppendaten. Die Benutzer- und Gruppendaten werden in Active Directory, OpenLDAP oder lokal im Betriebssystem der Maschine, auf der vCenter Single Sign On installiert ist, gespeichert.

Nach der Installation hat jede Instanz von vCenter Single Sign On die Identitätsquelle *Ihr_Domänenname*, z. B. „vsphere.local“. Diese Identitätsquelle ist für vCenter Single Sign On intern. Ein vCenter Single Sign On-Administrator kann Identitätsquellen hinzufügen, die Standardidentitätsquelle festlegen und Benutzer und Gruppen in der Identitätsquelle „vsphere.local“ erstellen.

Typen von Identitätsquellen

In vCenter Server-Versionen vor Version 5.1 wurden Active Directory und lokale Betriebssystembenutzer als Benutzer-Repositorys unterstützt. Deshalb konnten lokale Betriebssystembenutzer sich immer beim vCenter Server-System authentifizieren. vCenter Server 5.1 und 5.5 verwenden vCenter Single Sign On für die Authentifizierung. Eine Aufstellung der für vCenter Single Sign On 5.1 unterstützten Identitätsquellen finden Sie in der Dokumentation zu vSphere 5.1. vCenter Single Sign On 5.5 unterstützt die folgenden Typen von Benutzer-Repositorys als Identitätsquellen, unterstützt aber nur eine einzige standardmäßige Identitätsquelle.

- Active Directory-Versionen 2003 und später. Wird als **Active Directory (integrierte Windows-Authentifizierung)** im vSphere Web Client angezeigt. Mit vCenter Single Sign On können Sie eine einzelne Active Directory-Domäne als Identitätsquelle angeben. Die Domäne kann untergeordnete Domänen haben, oder es kann sich dabei um eine Gesamtstruktur-Stammdomäne handeln. Im VMware-KB-Artikel 2064250 werden Microsoft Active Directory-Vertrauensstellungen behandelt, die von vCenter Single Sign On unterstützt werden.
- Active Directory über LDAP. vCenter Single Sign On unterstützt mehrere Active Directory- über LDAP-Identitätsquellen. Dieser Identitätsquellentyp wird zur Gewährleistung der Kompatibilität zu dem in vSphere 5.1 enthaltenen vCenter Single Sign On-Dienst bereitgestellt. Er wird als **Active Directory als ein LDAP-Server** auf dem vSphere Web Client angezeigt.
- OpenLDAP Version 2.4 und höher. vCenter Single Sign On unterstützt mehrere OpenLDAP-Identitätsquellen. Wird als **OpenLDAP** auf dem vSphere Web Client angezeigt.
- Benutzer des lokalen Betriebssystems. Benutzer des lokalen Betriebssystems sind lokale Benutzer in dem Betriebssystem, unter dem der vCenter Single Sign On-Server läuft. Die Identitätsquelle des lokalen Betriebssystems existiert nur in einfachen vCenter Single Sign On-Serverbereitstellungen. In Bereitstellungen mit mehreren vCenter Single Sign On-Instanzen steht sie nicht zur Verfügung. Nur eine Identitätsquelle des lokalen Betriebssystems ist gestattet. Wird als **localos** auf dem vSphere Web Client angezeigt.

  Hinweis Verwenden Sie keine lokalen Betriebssystembenutzer, wenn sich der Platform Services Controller auf einer anderen Maschine als das vCenter Server-System befindet. Die Verwendung lokaler Betriebssystembenutzer kann bei einer eingebetteten Bereitstellung sinnvoll sein, wird jedoch nicht empfohlen.

- vCenter Single Sign On-Systembenutzer. Genau eine Systemidentitätsquelle, nämlich „vsphere.local“, wird bei der Installation von vCenter Single Sign On erstellt. Wird als **vsphere.local** auf dem vSphere Web Client angezeigt.

HINWEIS Es ist jeweils immer nur eine Standarddomäne vorhanden. Wenn sich ein Benutzer aus einer Nicht-Standarddomäne anmeldet, muss dieser Benutzer den Domänennamen (*DOMAIN**user*) hinzufügen, um erfolgreich authentifiziert zu werden.

Die vCenter Single Sign On-Identitätsquellen werden von vCenter Single Sign On-Administratorbenutzern verwaltet.

Sie können einer vCenter Single Sign On-Serverinstanz Identitätsquellen hinzufügen. Remoteidentitätsquellen sind auf Active Directory- und OpenLDAP-Server-Implementierungen beschränkt.

Weitere Informationen über vCenter Single Sign On finden Sie unter *vSphere-Sicherheit*.

Synchronisieren der Systemuhren im vSphere-Netzwerk

Stellen Sie sicher, dass auf allen Komponenten im vSphere-Netzwerk die Systemuhren synchronisiert sind. Wenn die Systemuhren der Maschinen im vSphere-Netzwerk nicht synchronisiert sind, werden SSL-Zertifikate, die zeitabhängig sind, bei der Kommunikation zwischen Netzwerkmaschinen möglicherweise nicht als gültig erkannt.

Nicht synchronisierte Systemuhren können Authentifizierungsprobleme verursachen, was zu einem Fehlschlag beim Installieren der vCenter Server Appliance führen bzw. verhindern kann, dass der vpxd-Dienst der vCenter Server Appliance gestartet wird.

Stellen Sie sicher, dass jede Windows-Hostmaschine, auf der eine vCenter-Komponente ausgeführt wird, mit dem NTP-Server synchronisiert wird. Weitere Informationen hierzu finden Sie im Knowledgebase-Artikel http://kb.vmware.com/kb/1318.

Synchronisieren der ESXi -Systemuhren mit einem NTP-Server

Bevor Sie vCenter Server installieren oder die vCenter Server Appliance bereitstellen, sollten Sie sicherstellen, dass die Systemuhren aller Maschinen im vSphere-Netzwerk synchronisiert sind.

Diese Aufgabe erläutert, wie Sie NTP über den vSphere Client einrichten. Sie können stattdessen den vCLI-Befehl `vicfg-ntp` verwenden. Weitere Informationen finden Sie in der *vSphere Command-Line Interface-Referenz*.

Vorgehensweise

1. Starten Sie den vSphere Client und stellen Sie eine Verbindung mit dem ESXi-Host her.
2. Klicken Sie auf der Registerkarte **Konfiguration** auf **Uhrzeitkonfiguration**.
3. Klicken Sie auf **Eigenschaften** und anschließend auf **Optionen**.
4. Wählen Sie **NTP-Einstellungen**.
5. Klicken Sie auf **Hinzufügen**.
6. Geben Sie im Dialogfeld „NTP-Server hinzufügen“ die IP-Adresse oder den vollqualifizierten Domänennamen des NTP-Servers ein, mit dem synchronisiert werden soll.
7. Klicken Sie auf **OK**.

   Die Hostuhrzeit wird mit dem NTP-Server synchronisiert.

Verwenden eines Benutzerkontos zur Ausführung von vCenter Server

Sie können das in Microsoft Windows integrierte Systemkonto oder ein Benutzerkonto zum Ausführen von vCenter Server verwenden. Mit einem Benutzerkonto können Sie die Windows-Authentifizierung für SQL Server aktivieren und für mehr Sicherheit sorgen.

Das Benutzerkonto muss ein Konto mit Administratorrechten für die lokale Maschine sein. Im Installationsassistenten wird der Kontoname in der Form *Domänenname\Benutzername* angegeben. Sie müssen die SQL Server-Datenbank konfigurieren, damit das Domänenkonto auf SQL Server zugreifen kann.

Das in Microsoft Windows integrierte Systemkonto verfügt über mehr Berechtigungen und Rechte auf dem Server als für das vCenter Server-System erforderlich ist, was zu Sicherheitsproblemen führen kann.

WICHTIG Wenn der vCenter Server-Dienst unter dem integrierten Systemkonto von Microsoft Windows ausgeführt wird, unterstützt vCenter Server 6.0 bei Verwendung von Microsoft SQL Server nur DSNs mit SQL Server-Authentifizierung.

Mit der Windows-Authentifizierung konfigurierte SQL Server-DSNs verwenden Sie dasselbe Benutzerkonto für den VMware VirtualCenter Management Webservices-Dienst und den DSN-Benutzer.

Selbst wenn Sie die Microsoft Windows-Authentifizierung nicht für SQL Server verwenden möchten oder Sie eine Oracle-Datenbank verwenden, sollten Sie ein lokales Benutzerkonto für das vCenter Server-System einrichten. Die einzige Anforderung besteht darin, dass das Benutzerkonto ein Konto mit Administratorrechten auf der lokalen Maschine ist und über die Berechtigung **Anmelden als Dienst** verfügt.

Installieren von vCenter Server auf IPv6-Maschinen

Ab vSphere 6.0 unterstützt vCenter Server Verbindungen zwischen vCenter Server und vCenter Server-Komponenten über entweder IPv4- oder IPv6-Adressen.

Eine gemischte Umgebung mit IPv4 und IPv6 wird nicht unterstützt. Wenn Sie vCenter Server in einer IPv6-Umgebung installieren, verwenden Sie den vollqualifizierten Domänennamen (FQDN) oder Hostnamen der Maschine, auf der Sie vCenter Server installieren. Bei einer reinen IPv4-Umgebung empfiehlt es sich, den vollqualifizierten Domänennamen (FQDN) oder Hostnamen der Maschine, auf der Sie vCenter Server installieren, zu verwenden, weil die IP-Adresse bei DHCP-Zuweisung sich ändern kann.

Ausführen des Installationsprogramms für vCenter Server über ein Netzlaufwerk

Sie können das Installationsprogramm für vCenter Server über ein Netzlaufwerk ausführen, die Software kann jedoch nicht auf einem Netzlaufwerk installiert werden.

In Windows können Sie die Installationsprogramme über ein Netzlaufwerk ausführen und die Software auf dem lokalen Computer installieren.

Erforderliche Informationen für die Installation von vCenter Server

Wenn Sie vCenter Server mit einem eingebetteten oder externen Platform Services Controller installieren, werden Sie vom Installationsassistenten zur Eingabe der Installationsinformationen aufgefordert.

Erforderliche Informationen für die Installation von vCenter Server mit einem eingebetteten Platform Services Controller

Der Installationsassistent für vCenter Server fordert Sie zur Eingabe von Installationsinformationen auf. Für den Fall, dass Sie das Produkt erneut installieren müssen, sollten Sie sich die eingegebenen Werte notieren.

Mithilfe dieses Arbeitsblatts können Sie die Informationen aufzeichnen, die Sie für die Installation von vCenter Server mit einem eingebetteten Platform Services Controller benötigen.

Tabelle 7-4. Erforderliche Informationen für die Installation von vCenter Server mit einem eingebetteten Platform Services Controller

Erforderliche Informationen		Standard	Ihr Eintrag
Systemname des lokalen Systems. Ein Systemname für die Verwaltung des lokalen Systems. Der Systemname muss ein FQDN sein. Geben Sie eine statische IP-Adresse an, falls kein DSN verfügbar ist.			
Neue vCenter Single Sign On-Domäne.	Domänenname	vsphere.local	
	Benutzername	Administrator	Während der Installation können Sie den Standardbenutzernamen nicht ändern.
	Kennwort für das vCenter Single Sign On-Administratorkonto. Das Kennwort muss aus mindestens acht Zeichen und maximal 20 Zeichen bestehen. Das Kennwort muss die folgenden Anforderungen erfüllen: ■ Es muss mindestens einen Großbuchstaben enthalten. ■ Es muss mindestens einen Kleinbuchstaben enthalten. ■ Es muss mindestens eine Zahl enthalten. ■ Es muss mindestens ein Sonderzeichen enthalten, beispielsweise ein kaufmännisches Und-Zeichen (&), ein Nummernzeichen (#) oder ein Prozentzeichen (%).		
	Site-Name. Ein Name für die vCenter Single Sign On-Site.		
vCenter Single Sign On-Domäne beitreten.	FQDN oder IP-Adresse für den Platform Services Controller.		
	HTTPS-Port für die Kommunikation mit einer vorhandenen vCenter Single Sign On-Domäne	443	
	Kennwort für das vCenter Single Sign On-Administratorkonto.		
	Treten Sie einer vorhandenen Site bei oder erstellen Sie eine neue Site. — Der Name der Site, der beigetreten werden soll, oder der Name der neuen Site.		

Tabelle 7-4. Erforderliche Informationen für die Installation von vCenter Server mit einem eingebetteten Platform Services Controller (Fortsetzung)

Erforderliche Informationen		Standard	Ihr Eintrag
vCenter Server-Dienstkontoinformationen. Hierbei kann es sich um ein Windows-Systemkonto oder ein benutzerdefiniertes Konto handeln.	Kontobenutzername Erforderlich, wenn Sie ein Benutzerdienstkonto verwenden.		
	Kontokennwort Erforderlich, wenn Sie ein Benutzerdienstkonto verwenden.		
Datenquellenname (DSN). Erforderlich, wenn Sie eine vorhandene externe Datenbank verwenden möchten. Nicht erforderlich, wenn Sie die im Lieferumfang enthaltene PostgreSQL-Datenbank verwenden möchten. Leerzeichen am Anfang und am Ende werden nicht unterstützt. Entfernen Sie die Leerzeichen am Anfang oder Ende des DSN.			
Datenbankbenutzername.	Erforderlich, wenn Sie eine vorhandene Datenbank verwenden möchten. Nicht erforderlich, wenn Sie die im Lieferumfang enthaltene PostgreSQL-Datenbank verwenden möchten. Nicht-ASCII-Zeichen werden nicht unterstützt.		
Datenbankkennwort.			
HTTP-Port.		80	
HTTPS-Port.		443	
Port für den Syslog-Dienst.		514	
TLS-Port für den Syslog-Dienst.		1514	
Port für Secure Token Service.		7444	
Auto Deploy-Management-Port.		6502	
Auto Deploy-Dienst-Port.		6501	
ESXi Dump Collector-Port.		6500	
ESXi-Taktsignal-Port.		902	
vSphere Web Client-Port.		9443	
Zielordner. ■ Der Ordner für die Installation von vCenter Server. ■ Der Ordner zum Speichern von Daten für vCenter Server mit einem eingebetteten Platform Services Controller. Die Installationspfade dürfen die folgenden Zeichen nicht enthalten: Nicht-ASCII-Zeichen, Kommas (,), Punkte (.), Ausrufezeichen (!), Nummernzeichen (#), At-Zeichen (@) und Prozentzeichen (%).		■ Der Standardinstallationsordner lautet `C:\Programme\VMware`. ■ Der Standardordner für die Datenspeicherung lautet `C:\ProgramData\VMware`.	

Erforderliche Informationen für die Installation eines Platform Services Controller

Wenn Sie vCenter Server mit einem externen Platform Services Controller installieren, werden Sie vom Installationsassistenten für den Platform Services Controller zur Eingabe der Installationsinformationen aufgefordert. Für den Fall, dass Sie das Produkt erneut installieren müssen, sollten Sie sich die eingegebenen Werte notieren.

Mithilfe dieses Arbeitsblatts können Sie die Informationen aufzeichnen, die Sie für die Installation eines externen Platform Services Controller benötigen.

Tabelle 7-5. Erforderliche Informationen für die Installation eines externen Platform Services Controller

Erforderliche Informationen		Standard	Ihr Eintrag
Systemname des lokalen Systems. Ein Systemname für die Verwaltung des lokalen Systems. Der Systemname muss ein FQDN sein. Geben Sie eine statische IP-Adresse an, falls kein DSN verfügbar ist.			
Neue vCenter Single Sign On-Domäne.	Domänenname	vsphere.local	
	Benutzername	Administrator	Während der Installation können Sie den Standardbenutzernamen nicht ändern.
	Kennwort für das vCenter Single Sign On-Administratorkonto. Das Kennwort muss aus mindestens acht Zeichen und maximal 20 Zeichen bestehen. Das Kennwort muss die folgenden Anforderungen erfüllen: ■ Es muss mindestens einen Großbuchstaben enthalten. ■ Es muss mindestens einen Kleinbuchstaben enthalten. ■ Es muss mindestens eine Zahl enthalten. ■ Es muss mindestens ein Sonderzeichen enthalten, beispielsweise ein kaufmännisches Und-Zeichen (&), ein Nummernzeichen (#) oder ein Prozentzeichen (%).		
	Site-Name. Ein Name für die vCenter Single Sign On-Site.		
vCenter Single Sign On-Domäne beitreten.	FQDN oder IP-Adresse für den Platform Services Controller		
	HTTPS-Port für die Kommunikation mit einer vorhandenen vCenter Single Sign On-Domäne	443	
	Kennwort für das vCenter Single Sign On-Administratorkonto.		
	Vorhandener Site beitreten oder neue Site erstellen Der Name der Site, der beigetreten werden soll, oder der Name der neuen Site.		
HTTP-Port.		80	
HTTPS-Port.		443	
Port für den Syslog-Dienst.		514	
TLS-Port für den Syslog-Dienst.		1514	

Tabelle 7-5. Erforderliche Informationen für die Installation eines externen Platform Services Controller (Fortsetzung)

Erforderliche Informationen	Standard	Ihr Eintrag
Port für Secure Token Service.	7444	
Zielordner. ■ Der Ordner für die Installation des Platform Services Controller. ■ Der Ordner zum Speichern von Daten für den Platform Services Controller. Die Installationspfade dürfen die folgenden Zeichen nicht enthalten: Nicht-ASCII-Zeichen, Kommas (,), Punkte (.), Ausrufezeichen (!), Nummernzeichen (#), At-Zeichen (@) und Prozentzeichen (%).	■ Der Standardinstallationsordner lautet `C:\Programme\VMware`. ■ Der Standardordner für die Datenspeicherung lautet `C:\ProgramData\VMware`.	

Erforderliche Informationen für die Installation von vCenter Server

Wenn Sie vCenter Server mit einem externen Platform Services Controller installieren, werden Sie vom Installationsassistenten für vCenter Server zur Eingabe der Installationsinformationen aufgefordert. Für den Fall, dass Sie das Produkt erneut installieren müssen, sollten Sie sich die eingegebenen Werte notieren.

Mithilfe dieses Arbeitsblatts können Sie die Informationen aufzeichnen, die Sie für die Installation von vCenter Server mit einem externen Platform Services Controller benötigen.

Tabelle 7-6. Erforderliche Informationen für die Installation von vCenter Server mit einem externen Platform Services Controller

<table>
<tr><th colspan="2">Erforderliche Informationen</th><th>Standardwert</th><th>Ihr Eintrag</th></tr>
<tr><td colspan="2">Systemname des lokalen Systems.
Ein Systemname für die Verwaltung des lokalen Systems. Der Systemname muss ein FQDN sein. Geben Sie eine statische IP-Adresse an, falls kein DSN verfügbar ist.</td><td></td><td></td></tr>
<tr><td rowspan="4">Informationen zu Single Sign On.</td><td>FQDN oder IP-Adresse für den Platform Services Controller.</td><td></td><td></td></tr>
<tr><td>Single Sign On-HTTPS-Port.</td><td>443</td><td></td></tr>
<tr><td>Single Sign On-Benutzername.</td><td></td><td></td></tr>
<tr><td>Single Sign On-Benutzerkennwort.</td><td></td><td></td></tr>
<tr><td rowspan="2">vCenter Server-Dienstkontoinformationen.
Hierbei kann es sich um ein Windows-Systemkonto oder ein benutzerdefiniertes Konto handeln.</td><td>Kontobenutzername
Erforderlich, wenn Sie ein Benutzerdienstkonto verwenden.</td><td></td><td></td></tr>
<tr><td>Kontokennwort
Erforderlich, wenn Sie ein Benutzerdienstkonto verwenden.</td><td></td><td></td></tr>
<tr><td colspan="2">Datenquellenname (DSN).
Erforderlich, wenn Sie eine vorhandene externe Datenbank verwenden. Nicht erforderlich, wenn Sie die im Lieferumfang enthaltene PostgreSQL-Datenbank verwenden. Leerzeichen am Anfang und am Ende werden nicht unterstützt. Entfernen Sie die Leerzeichen am Anfang oder Ende des DSN.</td><td></td><td></td></tr>
</table>

Tabelle 7-6. Erforderliche Informationen für die Installation von vCenter Server mit einem externen Platform Services Controller (Fortsetzung)

Erforderliche Informationen		Standardwert	Ihr Eintrag
Datenbankbenutzername.	Erforderlich, wenn Sie eine vorhandene Datenbank verwenden möchten. Nicht erforderlich, wenn Sie die im Lieferumfang enthaltene PostgreSQL-Datenbank verwenden möchten. Nicht-ASCII-Zeichen werden nicht unterstützt.		
Datenbankkennwort.			
HTTP-Port.		80	
HTTPS-Port.		443	
Port für den Syslog-Dienst.		514	
TLS-Port für den Syslog-Dienst.		1514	
Auto Deploy-Management-Port.		6502	
Auto Deploy-Dienst-Port.		6501	
ESXi Dump Collector-Port.		6500	
ESXi-Taktsignal-Port.		902	
vSphere Web Client-Port.		9443	
Zielordner. ■ Der Ordner für die Installation von vCenter Server. ■ Der Ordner zum Speichern von Daten für vCenter Server mit einem externen Platform Services Controller. Die Installationspfade dürfen die folgenden Zeichen nicht enthalten: Nicht-ASCII-Zeichen, Kommas (,), Punkte (.), Ausrufezeichen (!), Nummernzeichen (#), At-Zeichen (@) und Prozentzeichen (%).		■ Der Standardinstallationsordner lautet `C:\Programme\VMware`. ■ Der Standardordner für die Datenspeicherung lautet `C:\ProgramData\VMware`.	

Erforderliche Informationen für die Bereitstellung der vCenter Server Appliance

Wenn Sie die vCenter Server Appliance mit einem eingebetteten oder externen Platform Services Controller bereitstellen, werden Sie vom Installationsassistenten zur Eingabe der Bereitstellungsinformationen aufgefordert.

Erforderliche Informationen für die Bereitstellung der vCenter Server Appliance mit einem eingebetteten Platform Services Controller

Der Bereitstellungsassistent für die vCenter Server Appliance fordert Sie zur Eingabe der Bereitstellungsinformationen auf. Für den Fall, dass Sie das Produkt erneut installieren müssen, sollten Sie sich die eingegebenen Werte notieren.

Mithilfe dieses Arbeitsblatts können Sie die Informationen aufzeichnen, die Sie für die Bereitstellung einer vCenter Server Appliance mit einem eingebetteten Platform Services Controller benötigen.

Tabelle 7-7. Erforderliche Informationen für die Bereitstellung der vCenter Server Appliance mit einem eingebetteten Platform Services Controller

<table>
<tr><th colspan="2">Erforderliche Informationen</th><th>Standard</th><th>Ihr Eintrag</th></tr>
<tr><td colspan="2">FQDN oder IP-Adresse des ESXi-Hosts oder der vCenter Server-Instanz, auf dem bzw. auf der Sie vCenter Server Appliance bereitstellen.</td><td></td><td></td></tr>
<tr><td colspan="2">■ Wenn Sie den FQDN oder die IP-Adresse eines ESXi-Hosts verwenden, werden Sie vom Assistenten zur Eingabe eines Benutzernamens und eines Kennworts mit Administratorrechten für den ESXi-Host aufgefordert.
■ Wenn Sie den FQDN oder die IP-Adresse einer vCenter Server-Instanz verwenden, werden Sie vom Assistenten aufgefordert, einen Benutzernamen und ein Kennwort mit Administratorrechten für die vCenter Server-Instanz, das Datencenter oder den Datencenterordner sowie den Ressourcenpool eines ESXi-Hosts oder DRS-Clusters, auf dem die Appliance bereitgestellt werden soll, einzugeben.</td><td></td><td></td></tr>
<tr><td colspan="2">Name der vCenter Server Appliance</td><td>Beispiel: Muster-Appliance-Name</td><td></td></tr>
<tr><td colspan="2">Kennwort des Root-Benutzers des vCenter Server Appliance-Betriebssystems.
Das Kennwort muss aus mindestens acht Zeichen und maximal 20 Zeichen bestehen.
Das Kennwort muss die folgenden Anforderungen erfüllen:
■ Es muss mindestens einen Großbuchstaben enthalten.
■ Es muss mindestens einen Kleinbuchstaben enthalten.
■ Es muss mindestens eine Zahl enthalten.
■ Es muss mindestens ein Sonderzeichen enthalten, beispielweise ein Dollarzeichen ($), ein Nummernzeichen (#), ein At-Zeichen (@), einen Punkt (.) oder ein Ausrufezeichen (!).</td><td></td><td></td></tr>
<tr><td rowspan="2">Neue Single Sign On-Domäne.</td><td>Domänenname</td><td>vsphere.local</td><td></td></tr>
<tr><td>Benutzername</td><td>Administrator</td><td>Während der Installation können Sie den Standardbenutzernamen nicht ändern.</td></tr>
</table>

Tabelle 7-7. Erforderliche Informationen für die Bereitstellung der vCenter Server Appliance mit einem eingebetteten Platform Services Controller (Fortsetzung)

Erforderliche Informationen		Standard	Ihr Eintrag
	Kennwort für das vCenter Single Sign On-Administratorkonto. Das Kennwort muss aus mindestens acht Zeichen und maximal 20 Zeichen bestehen. Das Kennwort muss die folgenden Anforderungen erfüllen: ■ Es muss mindestens einen Großbuchstaben enthalten. ■ Es muss mindestens einen Kleinbuchstaben enthalten. ■ Es muss mindestens eine Zahl enthalten. ■ Es muss mindestens ein Sonderzeichen enthalten, beispielsweise ein kaufmännisches Und-Zeichen (&), ein Nummernzeichen (#) oder ein Prozentzeichen (%).		
	Site-Name. Ein Name für die vCenter Single Sign On-Site.		
Single Sign On-Domäne beitreten.	FQDN oder IP-Adresse für den Platform Services Controller.		
	Kennwort für das vCenter Single Sign On-Administratorkonto.		
	Portnummer	443	
	Site-Name		
Größe der vCenter Server Appliance. Die Optionen hängen von der Größe Ihrer vSphere-Umgebung ab: ■ Sehr klein (bis zu 10 Hosts, 100 virtuelle Maschinen) ■ Klein (bis zu 100 Hosts, 1,000 virtuelle Maschinen) ■ Mittel (bis zu 400 Hosts, 4,000 virtuelle Maschinen) ■ Groß (bis zu 1.000 Hosts, 10.000 virtuelle Maschinen)		Sehr klein (bis zu 10 Hosts, 100 virtuelle Maschinen	
Name des Datenspeichers, in dem die vCenter Server Appliance bereitgestellt wird			
Thin-Festplattenmodus aktivieren oder deaktivieren		Standardmäßig deaktiviert	
Oracle-Datenbankserver	Erforderlich, wenn Sie eine vorhandene Oracle-Datenbank verwenden möchten. Nicht erforderlich, wenn Sie die im Lieferumfang enthaltene PostgreSQL-Datenbank verwenden möchten. Nicht-ASCII-Zeichen werden nicht unterstützt.		
Oracle-Datenbankport			
Oracle-Datenbankinstanzname			
Datenbankbenutzername.			
Datenbankkennwort.			

Tabelle 7-7. Erforderliche Informationen für die Bereitstellung der vCenter Server Appliance mit einem eingebetteten Platform Services Controller (Fortsetzung)

Erforderliche Informationen		Standard	Ihr Eintrag
Netzwerkname			
Zuweisung der IP-Adresse Entweder IPv4 oder IPv6		IPv4	
Netzwerktyp Entweder DHCP oder statisch für IPv4; und DHCP oder statisch für IPv6.		DHCP	
Von den DHCP-Einstellungen zugewiesene IPv4-Adresse	FQDN Lassen Sie das Textfeld für den FQDN leer, falls in Ihrer Umgebung kein aktiviertes DNS vorhanden ist.		
	Aktivieren oder deaktivieren Sie SSH.	Standardmäßig deaktiviert	
Einstellungen für statische IPv4-Zuweisung	Netzwerkadresse		
	Systemname (FQDN oder IP-Adresse) Ein Systemname für die Verwaltung des lokalen Systems. Der Systemname muss ein FQDN sein. Geben Sie eine statische IP-Adresse an, wenn kein DNS verfügbar ist.		
	Subnetzmaske		
	Netzwerk-Gateway		
	Durch Kommas getrennte Netzwerk-DNS-Server		
	Aktivieren oder deaktivieren Sie SSH.	Standardmäßig deaktiviert	
Von den DHCP-Einstellungen zugewiesene IPv6-Adresse	FQDN Lassen Sie das Textfeld für den FQDN leer, falls in Ihrer Umgebung kein aktiviertes DNS vorhanden ist.		
	Aktivieren oder deaktivieren Sie SSH.	Standardmäßig deaktiviert	
Einstellungen für statische IPv6-Zuweisung	FQDN		
	Netzwerkadresse		
	Netzwerkpräfix		
	Netzwerk-Gateway		
	Durch Kommas getrennte Netzwerk-DNS-Server		

Tabelle 7-7. Erforderliche Informationen für die Bereitstellung der vCenter Server Appliance mit einem eingebetteten Platform Services Controller (Fortsetzung)

Erforderliche Informationen		Standard	Ihr Eintrag
	Aktivieren oder deaktivieren Sie SSH.	Standardmäßig deaktiviert	
Einstellungen für die Uhrzeitsynchronisierung Sie können die Uhrzeit der Appliance entweder mit der Uhrzeit des ESXi-Hosts synchronisieren oder NTP-Server verwenden.	Durch Kommas getrennte Namen der NTP-Server Erforderlich zur Verwendung von NTP-Servern für die Uhrzeitsynchronisierung		

Erforderliche Informationen für die Bereitstellung der Platform Services Controller -Appliance

Der Bereitstellungsassistent für den Platform Services Controller fordert Sie zur Eingabe der Bereitstellungsinformationen auf. Für den Fall, dass Sie das Produkt erneut installieren müssen, sollten Sie sich die eingegebenen Werte notieren.

Mithilfe dieses Arbeitsblatts können Sie die Informationen aufzeichnen, die Sie für die Bereitstellung eines externen Platform Services Controller benötigen.

Tabelle 7-8. Erforderliche Informationen für die Bereitstellung eines externen Platform Services Controller

Erforderliche Informationen	Standardwert	Ihr Eintrag
FQDN oder IP-Adresse des ESXi-Hosts oder der vCenter Server-Instanz, auf dem bzw. auf der Sie die Platform Services Controller-Appliance bereitstellen.		
■ Wenn Sie den FQDN oder die IP-Adresse eines ESXi-Hosts verwenden, werden Sie vom Assistenten zur Eingabe eines Benutzernamens und eines Kennworts mit Administratorrechten für den ESXi-Host aufgefordert. ■ Wenn Sie den FQDN oder die IP-Adresse einer vCenter Server-Instanz verwenden, werden Sie vom Assistenten aufgefordert, einen Benutzernamen und ein Kennwort mit Administratorrechten für die vCenter Server-Instanz, das Datencenter oder den Datencenterordner sowie den Ressourcenpool eines ESXi-Hosts oder DRS-Clusters, auf dem die Appliance bereitgestellt werden soll, einzugeben.		
Name der Platform Services Controller-Appliance	Beispiel: Muster-Appliance-Name	
Kennwort des Root-Benutzers des vCenter Server Appliance-Betriebssystems. Das Kennwort muss aus mindestens acht Zeichen und maximal 20 Zeichen bestehen. Das Kennwort muss die folgenden Anforderungen erfüllen: ■ Es muss mindestens einen Großbuchstaben enthalten. ■ Es muss mindestens einen Kleinbuchstaben enthalten. ■ Es muss mindestens eine Zahl enthalten. ■ Es muss mindestens ein Sonderzeichen enthalten, beispielweise ein Dollarzeichen ($), ein Nummernzeichen (#), ein At-Zeichen (@), einen Punkt (.) oder ein Ausrufezeichen (!).		

Tabelle 7-8. Erforderliche Informationen für die Bereitstellung eines externen Platform Services Controller (Fortsetzung)

Erforderliche Informationen		Standardwert	Ihr Eintrag
Neue Single Sign On-Domäne.	Domänenname	vsphere.local	
	Kennwort für das vCenter Single Sign On-Administratorkonto. Das Kennwort muss aus mindestens acht Zeichen und maximal 20 Zeichen bestehen. Das Kennwort muss die folgenden Anforderungen erfüllen: ■ Es muss mindestens einen Großbuchstaben enthalten. ■ Es muss mindestens einen Kleinbuchstaben enthalten. ■ Es muss mindestens eine Zahl enthalten. ■ Es muss mindestens ein Sonderzeichen enthalten, beispielsweise ein kaufmännisches Und-Zeichen (&), ein Nummernzeichen (#) oder ein Prozentzeichen (%).		
	Site-Name. Ein Name für die vCenter Single Sign On-Site.		
Single Sign On-Domäne beitreten.	FQDN oder IP-Adresse für den Platform Services Controller		
	Kennwort für das vCenter Single Sign On-Administratorkonto.		
	Portnummer	443	
	Site-Name		
Größe der Platform Services Controller-Appliance		Platform Services Controller	Die Standardoption kann nicht geändert werden. Die virtuelle Appliance, die Sie bereitstellen, weist 2 CPUs und 2 GB Arbeitsspeicher auf.
Name des Datenspeichers, auf dem die Platform Services Controller-Appliance bereitgestellt wird.			
Thin-Festplattenmodus aktivieren oder deaktivieren		Standardmäßig deaktiviert	
Netzwerkname			
Zuweisung der IP-Adresse Entweder IPv4 oder IPv6		IPv4	
Netzwerktyp Entweder DHCP oder statisch für IPv4; und DHCP oder statisch für IPv6.		DHCP	

Tabelle 7-8. Erforderliche Informationen für die Bereitstellung eines externen Platform Services Controller (Fortsetzung)

Erforderliche Informationen		Standardwert	Ihr Eintrag
Von den DHCP-Einstellungen zugewiesene IPv4-Adresse	FQDN Lassen Sie das Textfeld für den FQDN leer, falls in Ihrer Umgebung kein aktivierter DDNS vorhanden ist.		
	Aktivieren oder deaktivieren Sie SSH.	Standardmäßig deaktiviert	
Einstellungen für statische IPv4-Zuweisung	Netzwerkadresse		
	Systemname (FQDN oder IP-Adresse) Ein Systemname für die Verwaltung des lokalen Systems. Der Systemname muss ein FQDN sein. Geben Sie eine statische IP-Adresse an, wenn kein DNS verfügbar ist.		
	Subnetzmaske		
	Netzwerk-Gateway		
	Durch Kommas getrennte Netzwerk-DNS-Server		
	Aktivieren oder deaktivieren Sie SSH.	Standardmäßig deaktiviert	
Von den DHCP-Einstellungen zugewiesene IPv6-Adresse	FQDN Lassen Sie das Textfeld für den FQDN leer, falls Sie DNS nicht aktiviert haben.		
	Aktivieren oder deaktivieren Sie SSH.	Standardmäßig deaktiviert	
Einstellungen für statische IPv6-Zuweisung	FQDN		
	Netzwerkadresse		
	Netzwerkpräfix		
	Netzwerk-Gateway		
	Durch Kommas getrennte Netzwerk-DNS-Server		
	Aktivieren oder deaktivieren Sie SSH.	Standardmäßig deaktiviert	
Einstellungen für die Uhrzeitsynchronisierung Sie können die Uhrzeit der Appliance entweder mit der Uhrzeit des ESXi-Hosts synchronisieren oder NTP-Server verwenden.	Durch Kommas getrennte Namen der NTP-Server Erforderlich zur Verwendung von NTP-Servern für die Uhrzeitsynchronisierung		

Erforderliche Informationen für die Bereitstellung der vCenter Server Appliance

Der Bereitstellungsassistent für die vCenter Server Appliance fordert Sie zur Eingabe der Bereitstellungsinformationen auf. Für den Fall, dass Sie das Produkt erneut installieren müssen, sollten Sie sich die eingegebenen Werte notieren.

Mithilfe dieses Arbeitsblatts können Sie die Informationen aufzeichnen, die Sie für die Bereitstellung einer vCenter Server Appliance mit einem externen Platform Services Controller benötigen.

Tabelle 7-9. Erforderliche Informationen für die Bereitstellung der vCenter Server Appliance

Erforderliche Informationen	Standardwert	Ihr Eintrag
FQDN oder IP-Adresse des ESXi-Hosts oder der vCenter Server-Instanz, auf dem bzw. auf der Sie vCenter Server Appliance bereitstellen.		
■ Wenn Sie den FQDN oder die IP-Adresse eines ESXi-Hosts verwenden, werden Sie vom Assistenten zur Eingabe eines Benutzernamens und eines Kennworts mit Administratorrechten für den ESXi-Host aufgefordert. ■ Wenn Sie den FQDN oder die IP-Adresse einer vCenter Server-Instanz verwenden, werden Sie vom Assistenten aufgefordert, einen Benutzernamen und ein Kennwort mit Administratorrechten für die vCenter Server-Instanz, das Datencenter oder den Datencenterordner sowie den Ressourcenpool eines ESXi-Hosts oder DRS-Clusters, auf dem die Appliance bereitgestellt werden soll, einzugeben.		
Name der vCenter Server Appliance	Beispiel: Muster-Appliance-Name	
Kennwort des Root-Benutzers des vCenter Server Appliance-Betriebssystems. Das Kennwort muss aus mindestens acht Zeichen und maximal 20 Zeichen bestehen. Das Kennwort muss die folgenden Anforderungen erfüllen: ■ Es muss mindestens einen Großbuchstaben enthalten. ■ Es muss mindestens einen Kleinbuchstaben enthalten. ■ Es muss mindestens eine Zahl enthalten. ■ Es muss mindestens ein Sonderzeichen enthalten, beispielweise ein Dollarzeichen ($), ein Nummernzeichen (#), ein At-Zeichen (@), einen Punkt (.) oder ein Ausrufezeichen (!).		
FQDN oder IP-Adresse für den Platform Services Controller. Sie müssen den FQDN oder die IP-Adresse eines Platform Services Controller eingeben, den Sie bereits installiert oder bereitgestellt haben.		
Administratorkennwort für vCenter Single Sign On		
vCenter Single Sign On-HTTPS-Port.	443	
Größe der vCenter Server Appliance. Die Optionen hängen von der Größe Ihrer vSphere-Umgebung ab. ■ Sehr klein (bis zu 10 Hosts, 100 virtuelle Maschinen) ■ Klein (bis zu 100 Hosts, 1,000 virtuelle Maschinen) ■ Mittel (bis zu 400 Hosts, 4,000 virtuelle Maschinen) ■ Groß (bis zu 1.000 Hosts, 10.000 virtuelle Maschinen)	Sehr klein (bis zu 10 Hosts, 100 virtuelle Maschinen)	

Tabelle 7-9. Erforderliche Informationen für die Bereitstellung der vCenter Server Appliance (Fortsetzung)

Erforderliche Informationen		Standardwert	Ihr Eintrag
Name des Datenspeichers, in dem die vCenter Server Appliance bereitgestellt wird			
Thin-Festplattenmodus aktivieren oder deaktivieren		Standardmäßig deaktiviert	
Oracle-Datenbankserver	Nur erforderlich, wenn Sie eine vorhandene Oracle-Datenbank verwenden möchten. Nicht erforderlich, wenn Sie die im Lieferumfang enthaltene PostgreSQL-Datenbank verwenden. Nicht-ASCII-Zeichen werden nicht unterstützt.		
Oracle-Datenbankport			
Oracle-Datenbankinstanzname			
Datenbankbenutzername.			
Datenbankkennwort.			
Netzwerkname			
Zuweisung der IP-Adresse Entweder IPv4 oder IPv6		IPv4	
Netzwerktyp Entweder DHCP oder statisch für IPv4; und DHCP oder statisch für IPv6.		DHCP	
Von den DHCP-Einstellungen zugewiesene IPv4-Adresse	FQDN Lassen Sie das Textfeld für den FQDN leer, falls in Ihrer Umgebung kein aktiviertes DNS vorhanden ist.		
	Aktivieren oder deaktivieren Sie SSH.	Standardmäßig deaktiviert	
Einstellungen für statische IPv4-Zuweisung	Netzwerkadresse		
	Systemname (FQDN oder IP-Adresse) Ein Systemname für die Verwaltung des lokalen Systems. Der Systemname muss ein FQDN sein. Geben Sie eine statische IP-Adresse an, wenn kein DNS verfügbar ist.		
	Subnetzmaske		
	Netzwerk-Gateway		
	Durch Kommas getrennte Netzwerk-DNS-Server		
	Aktivieren oder deaktivieren Sie SSH.	Standardmäßig deaktiviert	
Von den DHCP-Einstellungen zugewiesene IPv6-Adresse	FQDN Lassen Sie das Textfeld für den FQDN leer, falls in Ihrer Umgebung kein aktiviertes DNS vorhanden ist.		
	Aktivieren oder deaktivieren Sie SSH.	Standardmäßig deaktiviert	
Einstellungen für statische IPv6-Zuweisung	FQDN		
	Netzwerkadresse		

Tabelle 7-9. Erforderliche Informationen für die Bereitstellung der vCenter Server Appliance (Fortsetzung)

Erforderliche Informationen		Standardwert	Ihr Eintrag
	Netzwerkpräfix		
	Netzwerk-Gateway		
	Durch Kommas getrennte Netzwerk-DNS-Server		
	Aktivieren oder deaktivieren Sie SSH.	Standardmäßig deaktiviert	
Einstellungen für die Uhrzeitsynchronisierung Sie können die Uhrzeit der Appliance entweder mit der Uhrzeit des ESXi-Hosts synchronisieren oder NTP-Server verwenden.	Durch Kommas getrennte Namen der NTP-Server Erforderlich zur Verwendung von NTP-Servern für die Uhrzeitsynchronisierung		

Installieren von vCenter Server auf einer virtuellen Windows-Maschine oder einem physischen Server 8

Sie können vCenter Server zum Verwalten Ihrer vSphere-Umgebung auf einer virtuellen Microsoft Windows-Maschine oder einem physischen Server installieren.

Laden Sie vor der Installation von vCenter Server die ISO-Datei herunter und mounten Sie sie auf der Windows-Hostmaschine, auf der Sie die Installation ausführen möchten, und starten Sie dann den Installationsassistenten.

Informationen zur den Anforderungen für vCenter Server finden Sie unter „Anforderungen für vCenter Server für Windows", auf Seite 27.

Informationen zu den Eingaben, die während der Installation von vCenter Server erforderlich sind, finden Sie unter „Erforderliche Informationen für die Installation von vCenter Server", auf Seite 232.

Nach der Installation von vCenter Server hat nur der Benutzer „administrator@*Ihr_Domänenname*" die Berechtigung, sich beim vCenter Server-System anzumelden.

Der Benutzer „administrator@*Ihr_Domänenname*" kann die folgenden Aufgaben ausführen:

- Hinzufügen einer Identitätsquelle, in der zusätzliche Benutzer und Gruppen definiert sind, in vCenter Single Sign On.
- Zuweisen von Rollen zu Benutzern und Gruppen, um ihnen Berechtigungen zuzuordnen.

Informationen zum Hinzufügen von Identitätsquellen und Zuweisen von Berechtigungen zu Benutzern und Gruppen finden Sie unter *vSphere-Sicherheit*.

Dieses Kapitel behandelt die folgenden Themen:

Laden Sie das Installationsprogramm für vCenter Server für Windows herunter.

Laden Sie das Installationsprogramm (ISO-Datei) für vCenter Server für Windows sowie die zugehörigen vCenter Server-Komponenten und Support-Tools herunter.

Voraussetzungen

Erstellen Sie ein „Mein VMware"-Konto unter https://my.vmware.com/web/vmware/.

Vorgehensweise

1 Laden Sie das Installationsprogramm für vCenter Server von der VMware-Website unter https://my.vmware.com/web/vmware/downloads herunter.

  vCenter Server ist eine Komponente von VMware vCloud Suite und VMware vSphere und unter „Datencenter- & Cloud-Infrastruktur“ aufgeführt.

2 Bestätigen Sie, dass „md5sum“ korrekt ist.

  Weitere Informationen hierzu finden Sie auf der VMware-Website im Thema „Using MD5 Checksums“ (Verwenden von MD5-Prüfsummen) unter http://www.vmware.com/download/md5.html.

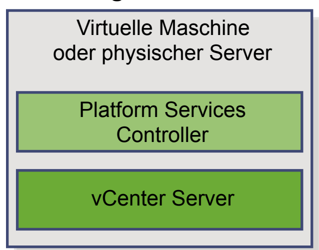
3 Mounten Sie das ISO-Image auf der virtuellen Windows-Maschine oder dem physischen Server, auf der/dem vCenter Server für Windows installiert werden soll.

Installieren von vCenter Server mit eingebettetem Platform Services Controller

Sie können vCenter Server, die vCenter Server-Komponenten und den Platform Services Controller auf einer einzelnen virtuelle Maschine oder einem physischen Server bereitstellen.

Nach der Bereitstellung von vCenter Server mit eingebettetem Platform Services Controller können Sie Ihre Topologie neu konfigurieren und auf vCenter Server mit externem Platform Services Controller umstellen. Dieser Vorgang ist unumkehrbar und Sie können nicht wieder auf vCenter Server mit eingebettetem Platform Services Controller zurücksetzen. Die vCenter Server-Instanz können Sie nur auf einen externen Platform Services Controller neu verweisen, für den die Replizierung der Infrastrukturdaten innerhalb derselben Domäne konfiguriert ist.

Abbildung 8-1. vCenter Server mit eingebettetem Platform Services Controller



WICHTIG Parallele Installationen von vCenter Server-Instanzen mit eingebetteten Platform Services Controller-Instanzen werden nicht unterstützt. Sie müssen die vCenter Server-Instanzen mit eingebetteten Platform Services Controller-Instanzen nacheinander installieren.

Voraussetzungen

- Überprüfen Sie, ob Ihr System die Mindestanforderungen an Software und Hardware erfüllt.
- Laden Sie das vCenter Server-Installationsprogramm herunter.
- Wenn Sie vSphere Web Client auf der Hostmaschine verwenden möchten, auf der Sie vCenter Server installieren, vergewissern Sie sich, dass die Adobe Flash Player-Version 11.9 oder höher auf dem System installiert ist.

Vorgehensweise

1 Doppelklicken Sie im Software-Installationsprogrammverzeichnis auf die Datei `autorun.exe`, um das Installationsprogramm zu starten.

2 Wählen Sie **vCenter Server für Windows** aus und klicken Sie auf **Installieren**.

3 Befolgen Sie die Anweisungen des Installationsassistenten zum Überprüfen der Begrüßungsseite und zum Akzeptieren der Lizenzvereinbarung.

4 Wählen Sie **vCenter Server mit eingebettetem Platform Services Controller** aus und klicken Sie auf **Weiter**.

5 Geben Sie den Systemnetzwerknamen ein, vorzugsweise einen FQDN, und klicken Sie auf **Weiter**.

Sie können auch eine IP-Adresse eingeben. Wenn Sie eine IP-Adresse eingeben, geben Sie eine statische IP-Adresse an.

WICHTIG Stellen Sie sicher, dass der FQDN bzw. die IP-Adresse, den/die Sie angeben, nicht geändert wird. Der Systemname kann nach der Bereitstellung nicht mehr geändert werden. Wenn der Systemname geändert wird, müssen Sie vCenter Server deinstallieren und dann neu installieren.

---

6 Erstellen Sie eine neue vCenter Single Sign On-Domäne oder treten Sie einer vorhandenen Domäne bei.

WICHTIG Sie können zwar einer vCenter Single Sign On-Domäne beitreten, aber Sie sollten vCenter Server mit eingebettetem Platform Services Controller als eigenständige Installation in Betracht ziehen und nicht für die Replizierung von Infrastrukturdaten verwenden.

Option	Beschreibung
Neue Single Sign On-Domäne erstellen	Erstellt einen neuen vCenter Single Sign On-Server. a Geben Sie den Domänennamen ein, z. B. **`vsphere.local`**. b Richten Sie das Kennwort für das vCenter Single Sign On-Administratorkonto ein. Dies ist das Kennwort für den Benutzer „administrator@*ihr_domänenname*“, wobei *ihr_domänenname* eine neue, von vCenter Single Sign On erstellte Domäne ist. Nach der Installation können Sie sich bei vCenter Single Sign On und bei vCenter Server als „adminstrator@*ihr_domänenname*“ anmelden. c Geben Sie den Websitenamen für vCenter Single Sign On ein. Der Site-Name spielt eine wichtige Rolle, wenn Sie vCenter Single Sign On an mehreren Standorten verwenden. Der Site-Name muss alphanumerische Zeichen enthalten. Wählen Sie Ihren eigenen Namen für die vCenter Single Sign On-Site. Der Name kann nach der Installation nicht mehr geändert werden. Nicht-ASCII-Zeichen bzw. Zeichen im hohen ASCII-Bereich werden in Site-Namen nicht unterstützt. Der Site-Name muss alphanumerische Zeichen und ein Komma (,), einen Punkt (.), ein Fragezeichen (?), einen Bindestrich (-), einen Unterstrich (_), ein Pluszeichen (+) oder ein Ist-gleich-Zeichen (=) enthalten.
Single Sign On-Domäne in einem vorhandenen Platform Services Controller beitreten	Fügt einen neuen vCenter Single Sign On-Server einer vCenter Single Sign On-Domäne in einem vorhandenen Platform Services Controller hinzu. Sie müssen die Informationen zum vCenter Single Sign On-Server angeben, dem Sie den neuen vCenter Single Sign On-Server hinzufügen. a Geben Sie den vollqualifizierten Domänennamen (Fully Qualified Domain Name, FQDN) oder die IP-Adresse des Platform Services Controller ein, der den hinzuzufügenden vCenter Single Sign On-Server enthält. b Geben Sie den HTTPS-Port für die Kommunikation mit dem Platform Services Controller ein. c Geben Sie das Kennwort des vCenter Single Sign On-Administratorkontos ein. d Klicken Sie auf **Weiter**. e Genehmigen Sie das von der Remotemaschine bereitgestellte Zertifikat. Sie müssen wählen, ob Sie eine vCenter Single Sign On-Site erstellen oder einer vorhandenen Site beitreten. f Wählen Sie, ob Sie eine vCenter Single Sign On-Site erstellen oder einer vorhandenen Site beitreten möchten.

7 Klicken Sie auf **Weiter**.

8 Wählen Sie das vCenter Server-Dienstkonto aus und klicken Sie auf **Weiter**.

Option	Beschreibung
Lokales Systemkonto von Windows verwenden	Der vCenter Server-Dienst wird unter dem lokalen Systemkonto von Windows ausgeführt. Diese Option hindert Sie daran, mithilfe der integrierten Windows-Authentifizierung eine Verbindung zu einer externen Datenbank herzustellen.
Benutzerdienstkonto angeben	Der vCenter Server-Dienst wird unter einem administrativen Benutzerkonto mit einem von Ihnen eingegebenen Benutzernamen und Kennwort ausgeführt.

WICHTIG Sie müssen Anmeldedaten für einen Benutzer eingeben, der sich in der lokalen Administratorengruppe befindet und der über das Recht **Anmelden als Dienst** verfügt.

9 Wählen Sie den gewünschten Datenbanktyp aus und klicken Sie auf **Weiter**.

Option	Beschreibung
Verwenden Sie eine eingebettete Datenbank (PostgreSQL)	vCenter Server verwendet die eingebettete PostgreSQL-Datenbank. Diese Datenbank ist für kleinere Bereitstellungen geeignet.
Externe Datenbank verwenden	vCenter Server verwendet eine vorhandene externe Datenbank. a Wählen Sie Ihre Datenbank aus der Liste mit den verfügbaren DSNs aus. b Geben Sie den Benutzernamen und das Kennwort für den DSN ein. Die Textfelder für den Namen und das Kennwort des Benutzers sind deaktiviert, falls Ihre Datenbank die Windows NT-Authentifizierung verwendet.

10 Übernehmen Sie für jede Komponente die Standardportnummer. Falls ein anderer Dienst die Standardports verwendet, geben Sie alternative Ports an und klicken Sie anschließend auf **Weiter**.

Vergewissern Sie sich, dass die Ports 80 und 443 frei und dediziert sind, damit vCenter Single Sign On diese Ports verwenden kann. Andernfalls verwenden Sie während der Installation benutzerdefinierte Ports.

11 (Optional) Ändern Sie die Standardzielordner und klicken Sie auf **Weiter**.

WICHTIG Verwenden Sie keine Ordnernamen, die mit einem Ausrufezeichen (!) enden.

12 Überprüfen Sie die Übersicht über die Installationseinstellungen und klicken Sie auf **Installieren**.

13 (Optional) Klicken Sie auf **vSphere Web Client starten**, um den vSphere Web Client zu starten, und melden Sie sich bei vCenter Server an.

14 Klicken Sie nach Abschluss der Installation auf **Beenden**.

vCenter Server, die vCenter Server-Komponenten und der Platform Services Controller werden installiert.

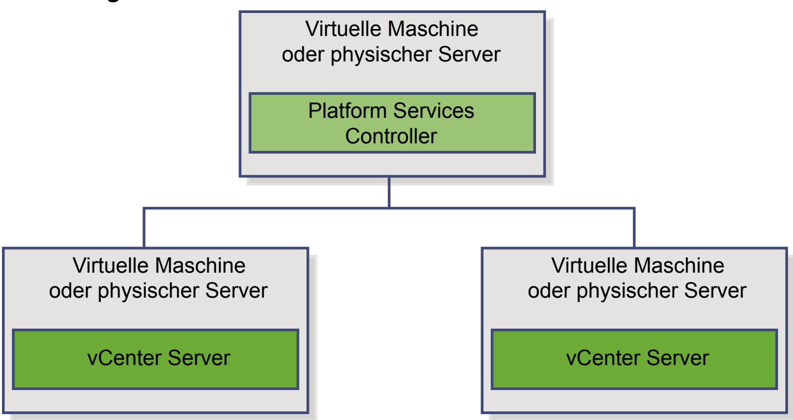
Installieren von vCenter Server mit einem externen Platform Services Controller

Sie können vCenter Server und den Platform Services Controller auf verschiedenen virtuellen Maschinen bzw. physischen Servern installieren.

Sie können Platform Services Controller und den vCenter Server voneinander trennen und auf verschiedenen virtuellen Maschinen bzw. physischen Servern installieren. Installieren Sie zuerst den Platform Services Controller, installieren Sie dann vCenter Server und die vCenter Server-Komponenten auf einer anderen virtuellen oder physischen Maschine und verbinden Sie vCenter Server mit dem Platform Services Controller. Sie können viele vCenter Server-Instanzen mit einem Platform Services Controller verbinden.

Wichtig Parallele Installationen von vCenter Server-Instanzen und Platform Services Controller-Instanzen werden nicht unterstützt. Sie müssen die Platform Services Controller- und vCenter Server-Instanzen nacheinander installieren.

Abbildung 8-2. vCenter Server mit einem externen Platform Services Controller



Nach der Bereitstellung von vCenter Server mit eingebettetem Platform Services Controller können Sie Ihre Topologie neu konfigurieren und auf vCenter Server mit externem Platform Services Controller umstellen. Dieser Vorgang ist unumkehrbar und Sie können nicht wieder auf vCenter Server mit eingebettetem Platform Services Controller zurücksetzen. Die vCenter Server-Instanz können Sie nur auf einen externen Platform Services Controller neu verweisen, für den die Replizierung der Infrastrukturdaten innerhalb derselben Domäne konfiguriert ist.

Wichtig Synchronisieren Sie die Uhren im vSphere-Netzwerk vor dem Installieren von vCenter Server mit einem externen Platform Services Controller. Ein Zeitversatz auf den virtuellen Maschinen oder physischen Servern, auf denen Sie den Platform Services Controller und vCenter Server installieren, kann einen Bereitstellungsfehler verursachen. Anweisungen zum Synchronisieren der Uhren auf dem vSphere-Netzwerk finden Sie unter „Synchronisieren der Systemuhren im vSphere-Netzwerk“, auf Seite 231.

Installieren eines Platform Services Controller auf einer Windows-Maschine

Um vCenter Server mit einem externen Platform Services Controller zu installieren, installieren Sie zuerst einen Platform Services Controller für Windows. Der Platform Services Controller enthält die üblichen Dienste wie vCenter Single Sign On und den Lizenzdienst, die von mehreren vCenter Server-Instanzen verwendet werden können.

Sie können mehrere Platform Services Controller-Instanzen installieren und in derselben vCenter Single Sign On-Domäne miteinander verbinden. Parallele (gleichzeitige) Installationen von Platform Services Controller-Instanzen werden nicht unterstützt. Sie müssen die Platform Services Controller-Instanzen nacheinander installieren.

WICHTIG Wenn Sie das VMCA-signierte Zertifikat durch ein von einer Zertifizierungsstelle (CA) signiertes Zertifikat ersetzen möchten, installieren Sie den Platform Services Controller zuerst, beziehen Sie dann VMCA in die Zertifikatskette mit ein und generieren Sie neue Zertifikate von VMCA, die durch die ganze Kette signiert sind. Sie können dann vCenter Server installieren. Informationen zum Verwalten von vCenter Server-Zertifikaten finden Sie in der Dokumentation *vSphere-Sicherheit*.

Voraussetzungen

- Überprüfen Sie, ob Ihr System die Mindestanforderungen an Software und Hardware erfüllt.
- Laden Sie das vCenter Server-Installationsprogramm herunter.
- Wenn Sie vSphere Web Client auf der Hostmaschine verwenden möchten, auf der Sie vCenter Server installieren, vergewissern Sie sich, dass die Adobe Flash Player-Version 11.9 oder höher auf dem System installiert ist.

Vorgehensweise

1. Doppelklicken Sie im Software-Installationsprogrammverzeichnis auf die Datei `autorun.exe`, um das Installationsprogramm zu starten.
2. Wählen Sie **vCenter Server für Windows** aus und klicken Sie auf **Installieren**.
3. Befolgen Sie die Anweisungen des Installationsassistenten zum Überprüfen der Begrüßungsseite und zum Akzeptieren der Lizenzvereinbarung.
4. Wählen Sie **Platform Services Controller** aus und klicken Sie auf **Weiter**.
5. Geben Sie den Systemnamen ein, vorzugsweise einen FQDN, und klicken Sie auf **Weiter**.

   Sie können auch eine IP-Adresse eingeben. Wenn Sie eine IP-Adresse eingeben, geben Sie eine statische IP-Adresse an.

   WICHTIG Wenn Sie einen FQDN oder eine IP-Adresse als Systemnamen des Platform Services Controller angeben, müssen Sie darauf achten, dass der FQDN oder die IP-Adresse nicht geändert wird. Wenn der FQDN oder die IP-Adresse der Hostmaschine geändert wird, müssen Sie den Platform Services Controller und die bei ihm registrierten vCenter Server-Instanzen neu installieren. Der FQDN oder die IP-Adresse des Platform Services Controller wird zum Generieren eines SSL-Zertifikats für die Hostmaschine mit dem Platform Services Controller verwendet.

   ---

6 Erstellen Sie eine neue vCenter Single Sign On-Domäne oder treten Sie einer vorhandenen Domäne bei.

Option	Beschreibung
Neue Single Sign On-Domäne erstellen	Erstellt einen neuen vCenter Single Sign On-Server. a Geben Sie den Domänennamen ein, z. B. **vsphere.local**. b Richten Sie das Kennwort für das vCenter Single Sign On-Administratorkonto ein. Dies ist das Kennwort für den Benutzer „administrator@*ihr_domänenname*“, wobei *ihr_domänenname* eine neue, von vCenter Single Sign On erstellte Domäne ist. Nach der Installation können Sie sich bei vCenter Single Sign On und bei vCenter Server als „adminstrator@*ihr_domänenname*“ anmelden. c Geben Sie den Websitenamen für vCenter Single Sign On ein. Der Site-Name spielt eine wichtige Rolle, wenn Sie vCenter Single Sign On an mehreren Standorten verwenden. Der Site-Name muss alphanumerische Zeichen enthalten. Wählen Sie Ihren eigenen Namen für die vCenter Single Sign On-Site. Der Name kann nach der Installation nicht mehr geändert werden. Nicht-ASCII-Zeichen bzw. Zeichen im hohen ASCII-Bereich werden in Site-Namen nicht unterstützt. Der Site-Name muss alphanumerische Zeichen und ein Komma (,), einen Punkt (.), ein Fragezeichen (?), einen Bindestrich (-), einen Unterstrich (_), ein Pluszeichen (+) oder ein Istgleich-Zeichen (=) enthalten.
Single Sign On-Domäne in einem vorhandenen Platform Services Controller beitreten	Fügt einen neuen vCenter Single Sign On-Server einer vCenter Single Sign On-Domäne in einem vorhandenen Platform Services Controller hinzu. Sie müssen die Informationen zum vCenter Single Sign On-Server angeben, dem Sie den neuen vCenter Single Sign On-Server hinzufügen. a Geben Sie den vollqualifizierten Domänennamen (Fully Qualified Domain Name, FQDN) oder die IP-Adresse des Platform Services Controller ein, der den hinzuzufügenden vCenter Single Sign On-Server enthält. b Geben Sie den HTTPS-Port für die Kommunikation mit dem Platform Services Controller ein. c Geben Sie das Kennwort des vCenter Single Sign On-Administratorkontos ein. d Klicken Sie auf **Weiter**. e Genehmigen Sie das von der Remotemaschine bereitgestellte Zertifikat. Sie müssen wählen, ob Sie eine vCenter Single Sign On-Site erstellen oder einer vorhandenen Site beitreten. f Wählen Sie, ob Sie eine vCenter Single Sign On-Site erstellen oder einer vorhandenen Site beitreten möchten.

Wenn Sie einer vorhandenen vCenter Single Sign On-Domäne beitreten, aktivieren Sie die Funktion „Erweiterter verknüpfter Modus“. Ihr Platform Services Controller repliziert Infrastrukturdaten an den beigetretenen vCenter Single Sign On-Server.

7 Klicken Sie auf **Weiter**.

8 Übernehmen Sie für jede Komponente die Standardportnummer. Falls ein anderer Dienst die Standardports verwendet, geben Sie alternative Ports an und klicken Sie anschließend auf **Weiter**.

Vergewissern Sie sich, dass die Ports 80 und 443 frei und dediziert sind, damit vCenter Single Sign On diese Ports verwenden kann. Andernfalls verwenden Sie während der Installation benutzerdefinierte Ports.

9 (Optional) Ändern Sie die Standardzielordner und klicken Sie auf **Weiter**.

WICHTIG Verwenden Sie keine Ordnernamen, die mit einem Ausrufezeichen (!) enden.

10 Überprüfen Sie die Übersicht über die Installationseinstellungen und klicken Sie auf **Installieren**.

11 Klicken Sie nach Abschluss der Installation auf **Beenden**.

Der Platform Services Controller wird installiert.

Weiter

Installieren Sie vCenter Server auf einer anderen virtuellen Windows-Maschine oder einem anderen physischen Server und registrieren Sie vCenter Server und die vCenter Server-Komponenten beim Platform Services Controller.

Installieren von vCenter Server und der vCenter Server -Komponenten

Nach dem Installieren eines Platform Services Controller auf einer Windows-Hostmaschine oder dem Bereitstellen einer Platform Services Controller-Appliance können Sie vCenter Server und die vCenter Server-Komponenten installieren und die vCenter Server-Instanz mit dem bereitgestellten Platform Services Controller verbinden.

Parallele (gleichzeitige) Installationen von vCenter Server-Instanzen werden nicht unterstützt. Wenn Sie mehrere vCenter Server-Instanzen installieren und bei demselben Platform Services Controller oder bei derselben Platform Services Controller-Appliance registrieren möchten, installieren Sie die vCenter Server-Instanzen nacheinander.

Voraussetzungen

- Überprüfen Sie, ob Ihr System die Mindestanforderungen an Software und Hardware erfüllt.
- Laden Sie das vCenter Server-Installationsprogramm herunter.
- Wenn Sie vSphere Web Client auf der Hostmaschine verwenden möchten, auf der Sie vCenter Server installieren, vergewissern Sie sich, dass die Adobe Flash Player-Version 11.9 oder höher auf dem System installiert ist.

Vorgehensweise

1 Doppelklicken Sie im Software-Installationsprogrammverzeichnis auf die Datei `autorun.exe`, um das Installationsprogramm zu starten.

2 Wählen Sie **vCenter Server für Windows** aus und klicken Sie auf **Installieren**.

3 Befolgen Sie die Anweisungen des Installationsassistenten zum Überprüfen der Begrüßungsseite und zum Akzeptieren der Lizenzvereinbarung.

4 Wählen Sie **vCenter Server** aus und klicken Sie auf **Weiter**.

5 Geben Sie den Systemnetzwerknamen ein, vorzugsweise eine statische IP-Adresse, und klicken Sie auf **Weiter**.

WICHTIG Der Name, den Sie eingeben, wird im SSL-Zertifikat des Systems codiert. Die Komponenten verwenden diesen Namen, wenn sie miteinander kommunizieren. Der Systemname muss eine statische IP-Adresse oder ein vollqualifizierter Domänenname (FQDN) sein. Stellen Sie sicher, dass der Systemname nicht geändert wird. Sie können den Systemnamen nach Abschluss der Installation nicht mehr ändern.

---

6 Geben Sie den Systemnamen des Platform Services Controller, den Sie schon installiert oder bereitgestellt haben, den HTTPS-Port, der für die Kommunikation mit dem vCenter Single Sign On-Server verwendet werden soll, und das Kennwort für vCenter Single Sign On an und klicken Sie auf **Weiter**.

   WICHTIG Stellen Sie sicher, dass Sie die IP-Adresse bzw. den vollqualifizierten Domänennamen verwenden, die/den Sie bei der Installation des Platform Services Controller angegeben haben. Wenn Sie den vollqualifizierten Domänennamen als Systemnamen des Platform Services Controller angegeben haben, können Sie keine IP-Adresse verwenden, und umgekehrt. Wenn sich ein Dienst von vCenter Server mit einem Dienst verbindet, der im Platform Services Controller ausgeführt wird, wird das Zertifikat verifiziert. Wenn die IP-Adresse oder der vollqualifizierte Domänenname geändert wird, schlägt die Prüfung fehl und vCenter Server kann sich nicht mit dem Platform Services Controller verbinden.

7 Genehmigen Sie das von der Remotemaschine bereitgestellte Zertifikat.

8 Wählen Sie das vCenter Server-Dienstkonto aus und klicken Sie auf **Weiter**.

Option	Beschreibung
Lokales Systemkonto von Windows verwenden	Der vCenter Server-Dienst wird unter dem lokalen Systemkonto von Windows ausgeführt. Diese Option hindert Sie daran, mithilfe der integrierten Windows-Authentifizierung eine Verbindung zu einer externen Datenbank herzustellen.
Benutzerdienstkonto angeben	Der vCenter Server-Dienst wird unter einem administrativen Benutzerkonto mit einem von Ihnen eingegebenen Benutzernamen und Kennwort ausgeführt.

   WICHTIG Sie müssen Anmeldedaten für einen Benutzer eingeben, der sich in der lokalen Administratorengruppe befindet und der über das Recht **Anmelden als Dienst** verfügt.

9 Wählen Sie den gewünschten Datenbanktyp aus und klicken Sie auf **Weiter**.

Option	Beschreibung
Verwenden Sie eine eingebettete Datenbank (PostgreSQL)	vCenter Server verwendet die eingebettete PostgreSQL-Datenbank. Diese Datenbank ist für kleinere Bereitstellungen geeignet.
Externe Datenbank verwenden	vCenter Server verwendet eine vorhandene externe Datenbank. a Wählen Sie Ihre Datenbank aus der Liste mit den verfügbaren DSNs aus. b Geben Sie den Benutzernamen und das Kennwort für den DSN ein. Die Textfelder für den Namen und das Kennwort des Benutzers sind deaktiviert, falls Ihre Datenbank die Windows NT-Authentifizierung verwendet.

10 Übernehmen Sie für jede Komponente die Standardportnummer. Falls ein anderer Dienst die Standardports verwendet, geben Sie alternative Ports an und klicken Sie anschließend auf **Weiter**.

11 (Optional) Ändern Sie die Standardzielordner und klicken Sie auf **Weiter**.

   WICHTIG Verwenden Sie keine Ordnernamen, die mit einem Ausrufezeichen (!) enden.

12 Überprüfen Sie die Übersicht über die Installationseinstellungen und klicken Sie auf **Installieren**.

13 (Optional) Klicken Sie auf **vSphere Web Client starten**, um den vSphere Web Client zu starten, und melden Sie sich bei vCenter Server an.

14 Klicken Sie nach Abschluss der Installation auf **Beenden**.

vCenter Server wird im Testmodus installiert. Sie können vCenter Server mit dem vSphere Web Client aktivieren. Informationen zum Aktivieren von vCenter Server finden Sie unter *vCenter Server und Hostverwaltung*.

Installieren von vCenter Server in einer Umgebung mit mehreren Netzwerkkarten

Wenn Sie vCenter Server mit einem externen Platform Services Controller in einer Umgebung mit mehreren Netzwerkkarten installieren möchten, müssen Sie die IP-Adressen oder FQDN, die Sie als Systemnetzwerknamen verwenden, notieren und aufbewahren.

Beispiel: Wenn Sie einen Platform Services Controller auf einer virtuellen Maschine und vCenter Server auf einer anderen virtuellen Maschine installieren möchten und jede virtuelle Maschine zwei Netzwerkkarten enthält, können Sie den folgenden Workflow verwenden:

1. Installieren Sie einen Platform Services Controller auf einer der virtuellen Maschinen und verwenden Sie eine der IP-Adressen oder FQDN als Systemnetzwerknamen.
2. Starten Sie auf der anderen virtuellen Maschine die Installation von vCenter Server und verwenden Sie eine der IP-Adressen oder FQDN als Systemnetzwerknamen.
3. Wenn Sie zur Eingabe des Systemnetzwerknamens des Platform Services Controller aufgefordert werden, geben Sie die IP-Adresse oder den vollständig qualifizierten Domänennamen (FQDN) ein, die/den Sie während der Installation des Platform Services Controller eingegeben haben.

   Wenn Sie die andere IP-Adresse bzw. den anderen FQDN des Platform Services Controller eingeben, wird eine Fehlermeldung angezeigt.
4. Nach Abschluss der Installation können Sie sich unter Verwendung einer der Netzwerkkarten-IP-Adressen oder FQDN von vCenter Server beim vSphere Web Client anmelden.

Bereitstellen der vCenter Server Appliance 9

Als Alternative zur Installation von vCenter Server auf einer virtuellen Windows-Maschine oder einem physischen Server können Sie die vCenter Server Appliance bereitstellen.

Laden Sie vor dem Bereitstellen der vCenter Server Appliance die ISO-Datei herunter und mounten Sie sie auf der Windows-Hostmaschine, auf der Sie die Bereitstellung ausführen möchten. Installieren Sie das Client-Integrations-Plug-In und starten Sie dann den Installationsassistenten.

Informationen zu den Anforderungen für die vCenter Server Appliance finden Sie unter „Anforderungen für die vCenter Server Appliance“, auf Seite 30.

Informationen zu den während der Bereitstellung der vCenter Server Appliance erforderlichen Eingaben finden Sie unter „Erforderliche Informationen für die Bereitstellung der vCenter Server Appliance“, auf Seite 237.

Für die vCenter Server Appliance gibt es die folgenden Standard-Benutzernamen:

- „root“ mit dem Betriebssystemkennwort, das Sie beim Bereitstellen der virtuellen Appliance eingeben.
- „administrator@*Ihr_Domänenname*“ mit dem vCenter Single Sign-On-Kennwort, das Sie beim Bereitstellen der virtuellen Appliance eingeben.

  Nach dem Bereitstellen der vCenter Server Appliance hat nur der Benutzer „administrator@*Ihr_Domänenname*“ die Berechtigung, sich beim vCenter Server-System anzumelden.

  Der Benutzer „administrator@*Ihr_Domänenname*“ kann wie folgt fortfahren:

  - Hinzufügen einer Identitätsquelle, in der zusätzliche Benutzer und Gruppen definiert sind, zu vCenter Single Sign On.
  - Weisen Sie den Benutzern und Gruppen Berechtigungen zu.

  Informationen zum Hinzufügen von Identitätsquellen und Zuweisen von Berechtigungen zu Benutzern und Gruppen finden Sie unter *vSphere-Sicherheit*.

Version 6.0 der vCenter Server Appliance wird mit der virtuellen Hardwareversion 8 bereitgestellt, die 32 virtuelle CPUs pro virtueller Maschine in ESXi unterstützt. In Abhängigkeit von den Hosts, die Sie mit der vCenter Server Appliance verwalten werden, sollten Sie möglicherweise ein Upgrade der ESXi -Hosts durchführen und die Hardwareversion der vCenter Server Appliance aktualisieren, um mehr virtuelle CPUs zu unterstützen:

- ESXi 5.5.x bietet Unterstützung bis zur virtuellen Hardwarevers 10 mit bis zu 64 virtuellen CPUs pro virtueller Maschine.

- ESXi 6.0 bietet Unterstützung bis zur virtuellen Hardwareversion 11 mit bis zu 128 virtuellen CPUs pro virtueller Maschine.

Wichtig Sie können die vCenter Server Appliance nicht mit dem vSphere Client oder vSphere Web Client bereitstellen. Bei der Bereitstellung der vCenter Server Appliance müssen Sie verschiedene Informationen eingeben, wie z. B. die Kennwörter des Betriebssystems und von vCenter Single Sign-On. Wenn Sie versuchen, die Appliance mit dem vSphere Client oder vSphere Web Client bereitzustellen, werden Sie nicht zur Eingabe dieser Informationen aufgefordert und die Bereitstellung schlägt fehl.

Informationen zum Aktualisieren der vCenter Server Appliance finden Sie unter *vSphere-Upgrade*.

Informationen zu Bestandslisten- und sonstigen Konfigurationsgrenzwerten in der vCenter Server Appliance finden Sie in der Dokumentation *Maximalwerte für die Konfiguration*.

Informationen zum Konfigurieren der vCenter Server Appliance finden Sie unter *vCenter Server Appliance-Konfiguration*.

Wichtig vCenter Server 6.0 unterstützt Verbindungen zwischen vCenter Server und vCenter Server-Komponenten über entweder IPv4- oder IPv6-Adressen. Eine gemischte Umgebung mit IPv4 und IPv6 wird nicht unterstützt. Wenn Sie die vCenter Server Appliance mit einer IPv6-Adresszuordnung einrichten möchten, stellen Sie sicher, dass der vollqualifizierte Domänenname (FQDN) oder der Hostname der Appliance verwendet wird. Bei einer IPv4-Umgebung empfiehlt es sich, den vollqualifizierten Domänennamen (FQDN) oder Hostnamen der Appliance zu verwenden, weil die IP-Adresse bei DHCP-Zuweisung sich ändern kann.

Dieses Kapitel behandelt die folgenden Themen:

Herunterladen des Installationsprogramms der vCenter Server Appliance

Laden Sie das ISO-Installationsprogramm der vCenter Server Appliance und das Client-Integrations-Plug-in herunter.

Voraussetzungen

Erstellen Sie ein „Mein VMware“-Konto unter https://my.vmware.com/web/vmware/.

Vorgehensweise

1 Laden Sie das Installationsprogramm der vCenter Server Appliance von der VMware-Website unter https://my.vmware.com/web/vmware/downloads herunter.

2 Bestätigen Sie, dass „md5sum“ korrekt ist.

   Weitere Informationen hierzu finden Sie auf der VMware-Website im Thema „Using MD5 Checksums“ (Verwenden von MD5-Prüfsummen) unter http://www.vmware.com/download/md5.html.

3 Mounten Sie das ISO-Image auf der virtuellen Windows-Maschine oder dem physischen Server, auf der bzw. dem das Client-Integrations-Plug-In zur Bereitstellung oder Aktualisierung der vCenter Server Appliance installiert werden soll.

   Wenn Sie eine virtuelle Windows-Maschine verwenden, können Sie das ISO-Image als Datenspeicher-ISO-Datei für das CD-/DVD-Laufwerk der virtuellen Maschine konfigurieren, indem Sie den vSphere Web Client verwenden. Siehe *vSphere-Administratorhandbuch für virtuelle Maschinen*.

Installieren des Client-Integrations-Plug-Ins

Sie müssen das Client-Integrations-Plug-In installieren, bevor Sie die vCenter Server Appliance bereitstellen oder aktualisieren können.

Voraussetzungen

Stellen Sie sicher, dass die `ISO`-Datei für vCenter Server Appliance heruntergeladen und gemountet wird.

Vorgehensweise

1 Wechseln Sie im Verzeichnis des Softwareinstallationsprogramms zum Verzeichnis `vcsa` und doppelklicken Sie auf `VMware-ClientIntegrationPlugin-6.0.0.exe`.

   Der Assistent Client-Integrations-Plug-In-Installation wird eingeblendet.

2 Klicken Sie auf der Begrüßungsseite auf **Weiter**.

3 Lesen und akzeptieren Sie die Endbenutzer-Lizenzvereinbarung und klicken Sie auf **Weiter**.

4 (Optional) Ändern Sie den Standardpfad zum Installationsordner des Client-Integrations-Plug-Ins und klicken Sie auf **Weiter**.

5 Prüfen Sie auf der Seite „Bereit zum Installieren des Plug-Ins“ des Assistenten die Informationen und klicken Sie auf **Installieren**.

6 Klicken Sie nach Abschluss der Installation auf **Beenden**.

Bereitstellen der vCenter Server Appliance mit einem eingebetteten Platform Services Controller

Wenn Sie die vCenter Server Appliance mit einem eingebetteten Platform Services Controller bereitstellen möchten, stellen Sie den Platform Services Controller und vCenter Server als eine Appliance bereit.

WICHTIG Parallele Bereitstellungen von vCenter Server Appliance-Instanzen mit eingebetteten Platform Services Controller-Instanzen werden nicht unterstützt. Sie müssen die vCenter Server Appliance-Instanzen mit eingebetteten Platform Services Controller-Instanzen in einer Sequenz bereitstellen.

Voraussetzungen

- Überprüfen Sie, ob Ihr System die Mindestanforderungen an Software und Hardware erfüllt.
- Laden Sie das vCenter Server Appliance-Installationsprogramm herunter.
- Installieren Sie das Client-Integrations-Plug-In.
- Überprüfen Sie, ob der ESXi-Host, auf dem Sie die vCenter Server Appliance bereitstellen, sich nicht im Sperr- oder im Wartungsmodus befindet.
- Stellen Sie sicher, dass Sie die richtigen Bereitstellungsinformationen für die Netzwerkeinstellungen vorbereitet haben. Details zu den bei der Bereitstellung erforderlichen Informationen finden Sie unter „Erforderliche Informationen für die Bereitstellung der vCenter Server Appliance mit einem eingebetteten Platform Services Controller“, auf Seite 237.

- Wenn Sie NTP-Server für die Uhrzeitsynchronisierung nutzen möchten, vergewissern Sie sich, dass die Uhrzeit zwischen den NTP-Servern und dem ESXi-Host synchronisiert ist.

Vorgehensweise

1. Doppelklicken Sie im Verzeichnis des Softwareinstallationsprogramms auf **vcsa-setup.html**.
2. Warten Sie bis zu drei Sekunden, bis der Browser das Client-Integrations-Plug-In erkennt, und lassen Sie bei Aufforderung zu, dass das Plug-In im Browser ausgeführt wird.
3. Klicken Sie auf der Startseite auf **Installieren**, um den Bereitstellungsassistenten für die vCenter Server Appliance zu starten.
4. Lesen und akzeptieren Sie die Lizenzvereinbarung und klicken Sie auf **Weiter**.
5. Stellen Sie eine Verbindung zu dem Zielserver her, auf dem Sie die vCenter Server Appliance-Appliance bereitstellen möchten, und klicken Sie auf **Weiter**.
   - Sie können eine Verbindung zu einem ESXi-Host herstellen, auf dem die Appliance bereitgestellt werden soll.
     a. Geben Sie den vollqualifizierten Domänennamen (FQDN) oder die IP-Adresse des ESXi-Hosts ein.
     b. Geben Sie Benutzernamen und Kennwort eines Benutzers mit Administratorrechten für den ESXi-Host ein, z. B. den Root-Benutzer.
   - Sie können eine Verbindung zu einer vCenter Server-Instanz herstellen, um die Appliance auf einem ESXi-Host oder DRS-Cluster über die vCenter Server-Bestandsliste bereitzustellen.
     a. Geben Sie den vollqualifizierten Domänennamen (FQDN) oder die IP-Adresse der vCenter Server-Instanz ein.
     b. Geben Sie Benutzernamen und Kennwort eines Benutzers mit Administratorrechten für die vCenter Server-Instanz ein, z. B. den Benutzer „administrator@*your_domain_name*“.
6. (Optional) Akzeptieren Sie die Zertifikatwarnung, falls vorhanden, indem Sie auf **Ja** klicken.
7. Wenn Sie die vCenter Server Appliance auf einer vCenter Server-Instanz bereitstellen, wählen Sie das Datencenter oder den Datencenterordner aus, das bzw. der den ESXi-Host oder DRS-Cluster enthält, auf dem Sie die Appliance bereitstellen möchten, und klicken Sie auf **Weiter**.

   Hinweis Sie müssen ein Datencenter oder einen Datencenterordner auswählen, das bzw. der mindestens einen ESXi-Host enthält, der sich nicht im Sperr- oder im Wartungsmodus befindet.

   ---
8. Wenn Sie die vCenter Server Appliance auf einer vCenter Server-Instanz bereitstellen, wählen Sie den Ressourcenpool eines ESXi-Hosts oder DRS-Clusters aus, auf dem Sie die Appliance bereitstellen möchten, und klicken Sie auf **Weiter**.

   Hinweis Wenn Sie einen Ressourcenpool eines Clusters auswählen, der sich nicht im DRS-Modus befindet, werden Sie vom Assistenten aufgefordert, einen ESXi-Host im Cluster auszuwählen.

   ---
9. Geben Sie auf der Einrichtungsseite der virtuellen Maschine den Namen der vCenter Server Appliance ein, legen Sie das Kennwort für den Root-Benutzer fest und klicken Sie auf **Weiter**.

   Das Kennwort muss mindestens acht Zeichen lang sein und eine Zahl, Groß- und Kleinbuchstaben und ein Sonderzeichen enthalten, z. B. ein Ausrufezeichen (!), ein Nummernzeichen (#), ein At-Zeichen (@) oder Klammern (()).
10. Wählen Sie auf der Seite „Bereitstellungstyp auswählen“ die Option **Installieren von vCenter Server mit eingebettetem Platform Services Controller** aus und klicken Sie auf **Weiter**.

    Mit dieser Option wird eine Appliance bereitgestellt, in der sowohl der Platform Services Controller als auch vCenter Server installiert sind.

11 Erstellen Sie eine neue vCenter Single Sign-On-Domäne oder treten Sie einer vorhandenen Domäne bei, und klicken Sie auf **Weiter**.

Wichtig Sie können zwar einer vCenter Single Sign On-Domäne beitreten, aber Sie sollten die vCenter Server Appliance mit eingebettetem Platform Services Controller als eigenständige Bereitstellung in Betracht ziehen und nicht für die Replizierung von Infrastrukturdaten verwenden.

Option	Beschreibung
Neue Single Sign On-Domäne erstellen	Erstellt einen neuen vCenter Single Sign On-Server. a Richten Sie das Kennwort für das vCenter Single Sign On-Administratorkonto ein. Dies ist das Kennwort für den Benutzer „administrator@*your_domain_name*", wobei *your_domain_name* eine neue, von vCenter Single Sign On erstellte Domäne ist.. Nach der Installation können Sie sich bei vCenter Single Sign On und bei vCenter Server als „adminstrator@*ihr_domänenname* anmelden. b Geben Sie den Domänennamen ein, z. B. **`vsphere.local`**. c Geben Sie den Websitenamen für vCenter Single Sign On ein. Der Site-Name spielt eine wichtige Rolle, wenn Sie vCenter Single Sign On an mehreren Standorten verwenden. Wählen Sie Ihren eigenen Namen für die vCenter Single Sign On-Site. Der Name kann nach der Installation nicht mehr geändert werden. Unterstützt werden alphanumerische Zeichen und Bindestrich (-).
Single Sign On-Domäne in einem vorhandenen Platform Services Controller beitreten	Fügt einen neuen vCenter Single Sign On-Server einer vCenter Single Sign On-Domäne in einem vorhandenen Platform Services Controller hinzu. Sie müssen die Informationen zum vCenter Single Sign On-Server angeben, dem Sie den neuen vCenter Single Sign On-Server hinzufügen. a Geben Sie den vollqualifizierten Domänennamen (Fully Qualified Domain Name, FQDN) oder die IP-Adresse des Platform Services Controller ein, der den hinzuzufügenden vCenter Single Sign On-Server enthält. b Geben Sie das Kennwort des vCenter Single Sign On-Administratorkontos ein. c Geben Sie den HTTPS-Port für die Kommunikation mit dem Platform Services Controller ein und klicken Sie auf **Weiter**. d Wählen Sie, ob Sie eine vCenter Single Sign On-Site erstellen oder einer vorhandenen Site beitreten möchten.

12 Wählen Sie auf der Seite „Appliance-Größe auswählen" des Assistenten die Größe der vCenter Server Appliance für Ihre vSphere-Bestandsliste aus und klicken Sie auf **Weiter**.

Option	Beschreibung
Sehr klein (bis zu 10 Hosts, 100 VMs)	Stellt eine Appliance mit 2 CPUs und 8 GB Arbeitsspeicher bereit.
Klein (bis zu 100 Hosts, 1.000 VMs)	Stellt eine Appliance mit 4 CPUs und 16 GB Arbeitsspeicher bereit.
Mittel (bis zu 400 Hosts, 4.000 VMs)	Stellt eine Appliance mit 8 CPUs und 24 GB Arbeitsspeicher bereit.
Groß (bis zu 1.000 Hosts, 10.000 VMs)	Stellt eine Appliance mit 16 CPUs und 32 GB Arbeitsspeicher bereit.

13 Wählen Sie aus der Liste mit den verfügbaren Datenspeichern den Speicherort für alle Konfigurationsdateien der virtuellen Maschine und alle virtuellen Festplatten aus. Aktivieren Sie optional Thin Provisioning, indem Sie **Thin-Festplattenmodus aktivieren** auswählen.

14 Wählen Sie den gewünschten Datenbanktyp aus und klicken Sie auf **Weiter**.

Option	Beschreibung
Verwenden Sie eine eingebettete Datenbank (PostgreSQL)	Konfiguriert vCenter Server in der Appliance für die Verwendung der eingebetteten PostgreSQL-Datenbank. Diese Datenbank ist für kleinere Bereitstellungen geeignet.
Oracle-Datenbank verwenden	Konfiguriert für vCenter Server in der Appliance die Verwendung einer vorhandenen externen Oracle-Datenbank. a Geben Sie die IP-Adresse oder den FQDN der Maschine ein, auf der die Oracle-Datenbank installiert ist. b Geben Sie den Port für die Kommunikation mit der Oracle-Datenbank ein. c Geben Sie den Namen der Datenbankinstanz ein. d Geben Sie den Benutzernamen und das Kennwort für die Datenbank ein. WICHTIG Vergewissern Sie sich, dass die angegebenen Anmeldedaten korrekt sind. Andernfalls schlägt die Bereitstellung möglicherweise fehl.

15 Richten Sie auf der Seite „Netzwerkeinstellungen" die Netzwerkeinstellungen ein.

Die IP-Adresse oder der FQDN der Appliance wird als Systemname verwendet. Es wird empfohlen, einen FQDN zu verwenden. Wenn Sie eine IP-Adresse verwenden möchten, verwenden Sie die Zuweisung einer statischen IP-Adresse für die Appliance, da die durch DHCP zugewiesenen IP-Adressen sich ändern könnten.

Option	Aktion
Netzwerk auswählen	Wählen Sie das Netzwerk aus, mit dem eine Verbindung hergestellt werden soll. Die im Dropdown-Menü angezeigten Netzwerke hängen von den Netzwerkeinstellungen des Zielservers ab. Wenn Sie die Appliance direkt auf einem ESXi-Host bereitstellen, werden nicht-flüchtige verteilte virtuelle Portgruppen nicht unterstützt und deshalb im Dropdown-Menü nicht angezeigt.
IP-Adressfamilie	Wählen Sie die IP-Version der Appliance aus. Sie können IPv4 oder IPv6 auswählen.
Netzwerktyp	Wählen Sie aus, wie die IP-Adresse der Appliance zugeteilt werden soll. ■ **Statisch** Sie werden aufgefordert, die IP-Adresse und die Netzwerkeinstellungen einzugeben. ■ **DHCP** Zum Zuteilen der IP-Adresse wird ein DHCP-Server verwendet. Wählen Sie diese Option nur, wenn ein DHCP-Server in Ihrer Umgebung verfügbar ist.
FQDN (Optional)	Geben Sie den gewünschten vollqualifizierten Domänennamen (FQDN) der Appliance ein. HINWEIS Wenn Sie die Verwendung von IPv6 mit dem Netzwerktyp DHCP auswählen, wird die FQDN-Option nicht angezeigt.

Wenn Sie eine IP-Adresse als Systemnamen verwenden, können Sie die IP-Adresse nicht ändern und die DNS-Einstellungen nach der Bereitstellung nicht aktualisieren.

16 Konfigurieren Sie die Uhrzeiteinstellungen in der Appliance. Wählen Sie optional **SSH aktivieren** aus, um die Verbindung zu sichern, und klicken Sie auf **Weiter**.

Option	Beschreibung
Appliance-Uhrzeit mit ESXi-Host synchronisieren	Aktiviert die regelmäßige Uhrzeitsynchronisierung, und VMware Tools legt die Uhrzeit des Gastbetriebssystems auf die Uhrzeit des ESXi-Hosts fest.
NTP-Server verwenden (durch Kommas getrennt)	Verwendet einen Netzwerkzeitprotokollserver (NTP) für die Synchronisierung der Uhrzeit. Bei Auswahl dieser Option müssen Sie die Namen der NTP-Server durch Kommas getrennt eingeben.

17 Überprüfen Sie auf der Seite „Bereit zum Abschließen“ die Bereitstellungseinstellungen für die vCenter Server Appliance und klicken Sie auf **Beenden**, um den Bereitstellungsvorgang abzuschließen.

18 (Optional) Klicken Sie nach Abschluss der Bereitstellung auf den Link **https://*vCenter_Server_Appliance-IP-Adresse*/vsphere-client**, um den vSphere Web Client zu starten, und melden Sie sich bei der vCenter Server-Instanz in der vCenter Server Appliance an.

19 Klicken Sie auf **Schließen**, um den Assistenten zu beenden.

Bereitstellen einer vCenter Server Appliance mit einem externen Platform Services Controller

Sie können eine vCenter Server Appliance mit einem externen Platform Services Controller bereitstellen. Auf diese Weise stellen Sie zwei verschiedene Appliances bereit.

Um den Platform Services Controller und die vCenter Server-Instanz als zwei verschiedene Appliances bereitzustellen, stellen Sie zuerst den Platform Services Controller bereit, stellen Sie dann vCenter Server und die vCenter Server-Komponenten als eine andere virtuelle Appliance bereit und registrieren Sie die vCenter Server Appliance beim Platform Services Controller.

WICHTIG Parallele Bereitstellungen von vCenter Server Appliance-Instanzen und Platform Services Controller-Appliances werden nicht unterstützt. Sie müssen die Platform Services Controller-Appliances und vCenter Server Appliance-Instanzen nacheinander bereitstellen.

WICHTIG Synchronisieren Sie die Uhren im vSphere-Netzwerk vor dem Bereitstellen einer vCenter Server Appliance mit einem externen Platform Services Controller. Ein Zeitversatz auf den virtuellen Maschinen kann einen Bereitstellungsfehler verursachen. Anweisungen zum Synchronisieren der Uhren auf dem vSphere-Netzwerk finden Sie unter „Synchronisieren der Systemuhren im vSphere-Netzwerk“, auf Seite 231.

Bereitstellen einer Platform Services Controller -Appliance

Wenn Sie die vCenter Server Appliance mit einem externen Platform Services Controller bereitstellen möchten, müssen Sie zuerst eine Platform Services Controller-Appliance bereitstellen. Die Platform Services Controller-Appliance enthält alle erforderlichen Dienste wie vCenter Single Sign On und den Lizenzdienst, die von mehreren vCenter Server-Instanzen gemeinsam verwendet werden können.

WICHTIG Sie können mehrere Platform Services Controller-Appliances bereitstellen und in derselben vCenter Single Sign On-Domäne miteinander verbinden. Parallele (gleichzeitige) Bereitstellungen von Platform Services Controller-Instanzen werden nicht unterstützt. Sie müssen die Platform Services Controller-Instanzen nacheinander bereitstellen.

Voraussetzungen

- Überprüfen Sie, ob Ihr System die Mindestanforderungen an Software und Hardware erfüllt.
- Laden Sie das vCenter Server Appliance-Installationsprogramm herunter.
- Installieren Sie das Client-Integrations-Plug-In.
- Überprüfen Sie, ob der ESXi-Host, auf dem Sie die Platform Services Controller-Appliance bereitstellen, sich nicht im Sperr- oder im Wartungsmodus befindet.
- Stellen Sie sicher, dass Sie die richtigen Bereitstellungsinformationen für die Netzwerkeinstellungen vorbereitet haben. Details zu den bei der Bereitstellung erforderlichen Informationen finden Sie unter „Erforderliche Informationen für die Bereitstellung der Platform Services Controller-Appliance“, auf Seite 241.

- Wenn Sie NTP-Server für die Uhrzeitsynchronisierung nutzen möchten, vergewissern Sie sich, dass die Uhrzeit zwischen den NTP-Servern und dem ESXi-Host synchronisiert ist.

Vorgehensweise

1 Doppelklicken Sie im Verzeichnis des Softwareinstallationsprogramms auf **vcsa-setup.html**.

2 Warten Sie bis zu drei Sekunden, bis der Browser das Client-Integrations-Plug-In erkennt, und lassen Sie bei Aufforderung zu, dass das Plug-In im Browser ausgeführt wird.

3 Klicken Sie auf der Startseite auf **Installieren**, um den Bereitstellungsassistenten für die vCenter Server Appliance zu starten.

4 Lesen und akzeptieren Sie die Lizenzvereinbarung und klicken Sie auf **Weiter**.

5 Stellen Sie eine Verbindung zu dem Zielserver her, auf dem Sie die Platform Services Controller-Appliance bereitstellen möchten, und klicken Sie auf **Weiter**.

   - Sie können eine Verbindung zu einem ESXi-Host herstellen, auf dem die Appliance bereitgestellt werden soll.

     a Geben Sie den vollqualifizierten Domänennamen (FQDN) oder die IP-Adresse des ESXi-Hosts ein.

     b Geben Sie Benutzernamen und Kennwort eines Benutzers mit Administratorrechten für den ESXi-Host ein, z. B. den Root-Benutzer.

   - Sie können eine Verbindung zu einer vCenter Server-Instanz herstellen, um die Appliance auf einem ESXi-Host oder DRS-Cluster über die vCenter Server-Bestandsliste bereitzustellen.

     a Geben Sie den vollqualifizierten Domänennamen (FQDN) oder die IP-Adresse der vCenter Server-Instanz ein.

     b Geben Sie Benutzernamen und Kennwort eines Benutzers mit Administratorrechten für die vCenter Server-Instanz ein, z. B. den Benutzer „administrator@*your_domain_name*“.

6 (Optional) Akzeptieren Sie die Zertifikatwarnung, falls vorhanden, indem Sie auf **Ja** klicken.

7 Wenn Sie den Platform Services Controller auf einer vCenter Server-Instanz bereitstellen, wählen Sie das Datencenter oder den Datencenterordner aus, das bzw. der den ESXi-Host oder DRS-Cluster enthält, auf dem Sie die Appliance bereitstellen möchten, und klicken Sie auf **Weiter**.

   Hinweis Sie müssen ein Datencenter oder einen Datencenterordner auswählen, das bzw. der mindestens einen ESXi-Host enthält, der sich nicht im Sperr- oder im Wartungsmodus befindet.

   ---

8 Wenn Sie den Platform Services Controller auf einer vCenter Server-Instanz bereitstellen, wählen Sie den Ressourcenpool eines ESXi-Hosts oder DRS-Clusters aus, auf dem Sie die Appliance bereitstellen möchten, und klicken Sie auf **Weiter**.

   Hinweis Wenn Sie einen Ressourcenpool eines Clusters auswählen, der sich nicht im DRS-Modus befindet, werden Sie vom Assistenten aufgefordert, einen ESXi-Host im Cluster auszuwählen.

   ---

9 Geben Sie auf der Seite „Virtuelle Maschine einrichten“ den Namen der Platform Services Controller-Appliance ein, legen Sie das Kennwort für den Root-Benutzer fest und klicken Sie auf **Weiter**.

   Das Kennwort muss mindestens acht Zeichen lang sein und eine Zahl, Groß- und Kleinbuchstaben und ein Sonderzeichen enthalten, z. B. ein Ausrufezeichen (!), ein Nummernzeichen (#), ein At-Zeichen (@) oder Klammern (()).

10 Wählen Sie auf der Seite „Bereitstellungstyp auswählen“ die Option **Platform Services Controller installieren** aus und klicken Sie auf **Weiter**.

11 Erstellen Sie eine neue vCenter Single Sign-On-Domäne oder treten Sie einer vorhandenen Domäne bei, und klicken Sie auf **Weiter**.

Option	Beschreibung
Neue Single Sign On-Domäne erstellen	Erstellt einen neuen vCenter Single Sign On-Server. a Richten Sie das Kennwort für das vCenter Single Sign On-Administratorkonto ein. Dies ist das Kennwort für den Benutzer „administrator@*your_domain_name*“, wobei *your_domain_name* eine neue, von vCenter Single Sign On erstellte Domäne ist.. Nach der Installation können Sie sich bei vCenter Single Sign On und bei vCenter Server als „adminstrator@*ihr_domänenname* anmelden. b Geben Sie den Domänennamen ein, z. B. `vsphere.local`. c Geben Sie den Websitenamen für vCenter Single Sign On ein. Der Site-Name spielt eine wichtige Rolle, wenn Sie vCenter Single Sign On an mehreren Standorten verwenden. Wählen Sie Ihren eigenen Namen für die vCenter Single Sign On-Site. Der Name kann nach der Installation nicht mehr geändert werden. Unterstützt werden alphanumerische Zeichen und Bindestrich (-).
Single Sign On-Domäne in einem vorhandenen Platform Services Controller beitreten	Fügt einen neuen vCenter Single Sign On-Server einer vCenter Single Sign On-Domäne in einem vorhandenen Platform Services Controller hinzu. Sie müssen die Informationen zum vCenter Single Sign On-Server angeben, dem Sie den neuen vCenter Single Sign On-Server hinzufügen. a Geben Sie den vollqualifizierten Domänennamen (Fully Qualified Domain Name, FQDN) oder die IP-Adresse des Platform Services Controller ein, der den hinzuzufügenden vCenter Single Sign On-Server enthält. b Geben Sie das Kennwort des vCenter Single Sign On-Administratorkontos ein. c Geben Sie den HTTPS-Port für die Kommunikation mit dem Platform Services Controller ein und klicken Sie auf **Weiter**. d Wählen Sie, ob Sie eine vCenter Single Sign On-Site erstellen oder einer vorhandenen Site beitreten möchten.

Wenn Sie einer vorhandenen vCenter Single Sign On-Domäne beitreten, aktivieren Sie die Funktion „Erweiterter verknüpfter Modus“. Ihr Platform Services Controller repliziert Infrastrukturdaten an den beigetretenen vCenter Single Sign On-Server.

12 Klicken Sie auf der Seite „Appliance-Größe auswählen“ des Assistenten auf **Weiter**.

Sie stellen eine Platform Services Controller-Appliance mit 2 CPUs und 2 GB Arbeitsspeicher bereit.

13 Wählen Sie aus der Liste mit den verfügbaren Datenspeichern den Speicherort für alle Konfigurationsdateien der virtuellen Maschine und alle virtuellen Festplatten aus. Aktivieren Sie optional Thin Provisioning, indem Sie **Thin-Festplattenmodus aktivieren** auswählen.

14 Richten Sie auf der Seite „Netzwerkeinstellungen“ die Netzwerkeinstellungen ein.

Die IP-Adresse oder der FQDN der Appliance wird als Systemname verwendet. Es wird empfohlen, einen FQDN zu verwenden. Wenn Sie eine IP-Adresse verwenden möchten, verwenden Sie die Zuweisung einer statischen IP-Adresse für die Appliance, da die durch DHCP zugewiesenen IP-Adressen sich ändern könnten.

Option	Aktion
Netzwerk auswählen	Wählen Sie das Netzwerk aus, mit dem eine Verbindung hergestellt werden soll. Die im Dropdown-Menü angezeigten Netzwerke hängen von den Netzwerkeinstellungen des Zielservers ab. Wenn Sie die Appliance direkt auf einem ESXi-Host bereitstellen, werden nicht-flüchtige verteilte virtuelle Portgruppen nicht unterstützt und deshalb im Dropdown-Menü nicht angezeigt.
IP-Adressfamilie	Wählen Sie die IP-Version der Appliance aus. Sie können IPv4 oder IPv6 auswählen.
Netzwerktyp	Wählen Sie aus, wie die IP-Adresse der Appliance zugeteilt werden soll. ■ **Statisch** Sie werden aufgefordert, die IP-Adresse und die Netzwerkeinstellungen einzugeben. ■ **DHCP** Zum Zuteilen der IP-Adresse wird ein DHCP-Server verwendet. Wählen Sie diese Option nur, wenn ein DHCP-Server in Ihrer Umgebung verfügbar ist.
FQDN (Optional)	Geben Sie den gewünschten vollqualifizierten Domänennamen (FQDN) der Appliance ein. HINWEIS Wenn Sie die Verwendung von IPv6 mit dem Netzwerktyp DHCP auswählen, wird die FQDN-Option nicht angezeigt.

Wenn Sie eine IP-Adresse als Systemnamen verwenden, können Sie die IP-Adresse nicht ändern und die DNS-Einstellungen nach der Bereitstellung nicht aktualisieren.

15 Konfigurieren Sie die Uhrzeiteinstellungen in der Appliance. Wählen Sie optional **SSH aktivieren** aus, um die Verbindung zu sichern, und klicken Sie auf **Weiter**.

Option	Beschreibung
Appliance-Uhrzeit mit ESXi-Host synchronisieren	Aktiviert die regelmäßige Uhrzeitsynchronisierung, und VMware Tools legt die Uhrzeit des Gastbetriebssystems auf die Uhrzeit des ESXi-Hosts fest.
NTP-Server verwenden (durch Kommas getrennt)	Verwendet einen Netzwerkzeitprotokollserver (NTP) für die Synchronisierung der Uhrzeit. Bei Auswahl dieser Option müssen Sie die Namen der NTP-Server durch Kommas getrennt eingeben.

16 Überprüfen Sie auf der Seite „Bereit zum Abschließen“ die Bereitstellungseinstellungen für die vCenter Server Appliance und klicken Sie auf **Beenden**, um den Bereitstellungsvorgang abzuschließen.

Weiter

Sie können jetzt die vCenter Server Appliance bereitstellen und mit der Platform Services Controller-Appliance verbinden.

Bereitstellen der vCenter Server Appliance

Stellen Sie die vCenter Server Appliance nach dem Bereitstellen der Platform Services Controller-Appliance oder Installieren eines Platform Services Controller auf einer virtuellen Windows-Maschine oder einem physischen Server bereit.

WICHTIG Parallele Bereitstellungen von vCenter Server Appliance-Instanzen werden nicht unterstützt. Wenn Sie mehrere vCenter Server Appliance-Instanzen bereitstellen und bei demselben Platform Services Controller oder bei derselben Platform Services Controller-Appliance registrieren möchten, stellen Sie die vCenter Server Appliance-Instanzen nacheinander bereit.

Voraussetzungen

- Überprüfen Sie, ob Ihr System die Mindestanforderungen an Software und Hardware erfüllt.
- Laden Sie das vCenter Server Appliance-Installationsprogramm herunter.

- Installieren Sie das Client-Integrations-Plug-In.
- Überprüfen Sie, ob der ESXi-Host, auf dem Sie die vCenter Server Appliance bereitstellen, sich nicht im Sperr- oder im Wartungsmodus befindet.
- Stellen Sie sicher, dass Sie die richtigen Bereitstellungsinformationen für die Netzwerkeinstellungen vorbereitet haben. Details zu den bei der Bereitstellung erforderlichen Informationen finden Sie unter „Erforderliche Informationen für die Bereitstellung der vCenter Server Appliance“, auf Seite 244.
- Wenn Sie NTP-Server für die Uhrzeitsynchronisierung nutzen möchten, vergewissern Sie sich, dass die Uhrzeit zwischen den NTP-Servern und dem ESXi-Host synchronisiert ist.

Vorgehensweise

1. Doppelklicken Sie im Verzeichnis des Softwareinstallationsprogramms auf **vcsa-setup.html**.
2. Warten Sie bis zu drei Sekunden, bis der Browser das Client-Integrations-Plug-In erkennt, und lassen Sie bei Aufforderung zu, dass das Plug-In im Browser ausgeführt wird.
3. Klicken Sie auf der Startseite auf **Installieren**, um den Bereitstellungsassistenten für die vCenter Server Appliance zu starten.
4. Lesen und akzeptieren Sie die Lizenzvereinbarung und klicken Sie auf **Weiter**.
5. Stellen Sie eine Verbindung zu dem Zielserver her, auf dem Sie die vCenter Server Appliance-Appliance bereitstellen möchten, und klicken Sie auf **Weiter**.
   - Sie können eine Verbindung zu einem ESXi-Host herstellen, auf dem die Appliance bereitgestellt werden soll.
     a. Geben Sie den vollqualifizierten Domänennamen (FQDN) oder die IP-Adresse des ESXi-Hosts ein.
     b. Geben Sie Benutzernamen und Kennwort eines Benutzers mit Administratorrechten für den ESXi-Host ein, z. B. den Root-Benutzer.
   - Sie können eine Verbindung zu einer vCenter Server-Instanz herstellen, um die Appliance auf einem ESXi-Host oder DRS-Cluster über die vCenter Server-Bestandsliste bereitzustellen.
     a. Geben Sie den vollqualifizierten Domänennamen (FQDN) oder die IP-Adresse der vCenter Server-Instanz ein.
     b. Geben Sie Benutzernamen und Kennwort eines Benutzers mit Administratorrechten für die vCenter Server-Instanz ein, z. B. den Benutzer „administrator@*your_domain_name*“.
6. (Optional) Akzeptieren Sie die Zertifikatwarnung, falls vorhanden, indem Sie auf **Ja** klicken.
7. Wenn Sie die vCenter Server Appliance auf einer vCenter Server-Instanz bereitstellen, wählen Sie das Datencenter oder den Datencenterordner aus, das bzw. der den ESXi-Host oder DRS-Cluster enthält, auf dem Sie die Appliance bereitstellen möchten, und klicken Sie auf **Weiter**.

   Hinweis Sie müssen ein Datencenter oder einen Datencenterordner auswählen, das bzw. der mindestens einen ESXi-Host enthält, der sich nicht im Sperr- oder im Wartungsmodus befindet.

8. Wenn Sie die vCenter Server Appliance auf einer vCenter Server-Instanz bereitstellen, wählen Sie den Ressourcenpool eines ESXi-Hosts oder DRS-Clusters aus, auf dem Sie die Appliance bereitstellen möchten, und klicken Sie auf **Weiter**.

   Hinweis Wenn Sie einen Ressourcenpool eines Clusters auswählen, der sich nicht im DRS-Modus befindet, werden Sie vom Assistenten aufgefordert, einen ESXi-Host im Cluster auszuwählen.

9 Geben Sie auf der Einrichtungsseite der virtuellen Maschine den Namen der vCenter Server Appliance ein, legen Sie das Kennwort für den Root-Benutzer fest und klicken Sie auf **Weiter**.

   Das Kennwort muss mindestens acht Zeichen lang sein und eine Zahl, Groß- und Kleinbuchstaben und ein Sonderzeichen enthalten, z. B. ein Ausrufezeichen (!), ein Nummernzeichen (#), ein At-Zeichen (@) oder Klammern (()).

10 Wählen Sie auf der Seite „Bereitstellungstyp auswählen" die Option **vCenter Server installieren** aus und klicken Sie auf **Weiter**.

11 Geben Sie den Systemnamen eines Platform Services Controller, den Sie schon installiert haben, an, geben Sie das Kennwort für vCenter Single Sign On ein und klicken Sie auf **Weiter**.

   Wenn Sie eine Platform Services Controller-Appliance bereitgestellt haben, geben Sie die IP-Adresse der neu bereitgestellten Appliance an. Wenn Sie einen Platform Services Controller unter Windows installiert haben, geben Sie den Systemnamen der Hostmaschine an, auf der Sie den Platform Services Controller installiert haben.

12 Wählen Sie auf der Seite „Appliance-Größe auswählen" des Assistenten die Größe der vCenter Server Appliance in Abhängigkeit von der Größe der vSphere-Bestandsliste aus und klicken Sie auf **Weiter**.

Option	Beschreibung
Sehr klein (bis zu 10 Hosts, 100 VMs)	Stellt eine Appliance mit 2 CPUs und 8 GB Arbeitsspeicher bereit.
Klein (bis zu 100 Hosts, 1.000 VMs)	Stellt eine Appliance mit 4 CPUs und 16 GB Arbeitsspeicher bereit.
Mittel (bis zu 400 Hosts, 4.000 VMs)	Stellt eine Appliance mit 8 CPUs und 24 GB Arbeitsspeicher bereit.
Groß (bis zu 1.000 Hosts, 10.000 VMs)	Stellt eine Appliance mit 16 CPUs und 32 GB Arbeitsspeicher bereit.

13 Wählen Sie aus der Liste mit den verfügbaren Datenspeichern den Speicherort für alle Konfigurationsdateien der virtuellen Maschine und alle virtuellen Festplatten aus. Aktivieren Sie optional Thin Provisioning, indem Sie **Thin-Festplattenmodus aktivieren** auswählen.

14 Wählen Sie den gewünschten Datenbanktyp aus und klicken Sie auf **Weiter**.

Option	Beschreibung
Verwenden Sie eine eingebettete Datenbank (PostgreSQL)	Konfiguriert vCenter Server in der Appliance für die Verwendung der eingebetteten PostgreSQL-Datenbank. Diese Datenbank ist für kleinere Bereitstellungen geeignet.
Oracle-Datenbank verwenden	Konfiguriert für vCenter Server in der Appliance die Verwendung einer vorhandenen externen Oracle-Datenbank. a Geben Sie die IP-Adresse oder den FQDN der Maschine ein, auf der die Oracle-Datenbank installiert ist. b Geben Sie den Port für die Kommunikation mit der Oracle-Datenbank ein. c Geben Sie den Namen der Datenbankinstanz ein. d Geben Sie den Benutzernamen und das Kennwort für die Datenbank ein. WICHTIG Vergewissern Sie sich, dass die angegebenen Anmeldedaten korrekt sind. Andernfalls schlägt die Bereitstellung möglicherweise fehl.

15 Richten Sie auf der Seite „Netzwerkeinstellungen" die Netzwerkeinstellungen ein.

   Die IP-Adresse oder der FQDN der Appliance wird als Systemname verwendet. Es wird empfohlen, einen FQDN zu verwenden. Wenn Sie eine IP-Adresse verwenden möchten, verwenden Sie die Zuweisung einer statischen IP-Adresse für die Appliance, da die durch DHCP zugewiesenen IP-Adressen sich ändern könnten.

Option	Aktion
Netzwerk auswählen	Wählen Sie das Netzwerk aus, mit dem eine Verbindung hergestellt werden soll. Die im Dropdown-Menü angezeigten Netzwerke hängen von den Netzwerkeinstellungen des Zielservers ab. Wenn Sie die Appliance direkt auf einem ESXi-Host bereitstellen, werden nicht-flüchtige verteilte virtuelle Portgruppen nicht unterstützt und deshalb im Dropdown-Menü nicht angezeigt.
IP-Adressfamilie	Wählen Sie die IP-Version der Appliance aus. Sie können IPv4 oder IPv6 auswählen.
Netzwerktyp	Wählen Sie aus, wie die IP-Adresse der Appliance zugeteilt werden soll. ■ **Statisch** Sie werden aufgefordert, die IP-Adresse und die Netzwerkeinstellungen einzugeben. ■ **DHCP** Zum Zuteilen der IP-Adresse wird ein DHCP-Server verwendet. Wählen Sie diese Option nur, wenn ein DHCP-Server in Ihrer Umgebung verfügbar ist.
FQDN (Optional)	Geben Sie den gewünschten vollqualifizierten Domänennamen (FQDN) der Appliance ein. HINWEIS Wenn Sie die Verwendung von IPv6 mit dem Netzwerktyp DHCP auswählen, wird die FQDN-Option nicht angezeigt.

Wenn Sie eine IP-Adresse als Systemnamen verwenden, können Sie die IP-Adresse nicht ändern und die DNS-Einstellungen nach der Bereitstellung nicht aktualisieren.

16 Konfigurieren Sie die Uhrzeiteinstellungen in der Appliance. Wählen Sie optional **SSH aktivieren** aus, um die Verbindung zu sichern, und klicken Sie auf **Weiter**.

Option	Beschreibung
Appliance-Uhrzeit mit ESXi-Host synchronisieren	Aktiviert die regelmäßige Uhrzeitsynchronisierung, und VMware Tools legt die Uhrzeit des Gastbetriebssystems auf die Uhrzeit des ESXi-Hosts fest.
NTP-Server verwenden (durch Kommas getrennt)	Verwendet einen Netzwerkzeitprotokollserver (NTP) für die Synchronisierung der Uhrzeit. Bei Auswahl dieser Option müssen Sie die Namen der NTP-Server durch Kommas getrennt eingeben.

17 Überprüfen Sie auf der Seite „Bereit zum Abschließen“ die Bereitstellungseinstellungen für die vCenter Server Appliance und klicken Sie auf **Beenden**, um den Bereitstellungsvorgang abzuschließen.

18 (Optional) Klicken Sie nach Abschluss der Bereitstellung auf den Link **https://*vCenter_Server_Appliance-IP-Adresse*/vsphere-client**, um den vSphere Web Client zu starten, und melden Sie sich bei der vCenter Server-Instanz in der vCenter Server Appliance an.

19 Klicken Sie auf **Schließen**, um den Assistenten zu beenden.

Fehlerbehebung bei der vCenter Server -Installation oder -Bereitstellung

10

Die Themen zur Fehlerbehebung bei der vCenter Server-Installation oder -Bereitstellung enthalten Lösungen für Probleme, auf die Sie bei der vCenter Server-Installation oder dem vCenter Server Appliance-Bereitstellungsprozess stoßen können.

Dieses Kapitel behandelt die folgenden Themen:

Erfassen von Protokollen für die Fehlerbehebung bei einer vCenter Server -Installation oder einem Upgrade

Sie können Installations- oder Upgrade-Protokolldateien für vCenter Server erfassen. Wenn eine Installation oder ein Upgrade fehlschlägt, kann die Prüfung der Protokolldateien Sie bei der Identifizierung der Fehlerquelle unterstützen.

Sie können die Installationsassistent-Methode oder die manuelle Methode wählen, um Protokolldateien für den Fall eines Installationsfehlers bei vCenter Server für Windows zu speichern und wiederherzustellen.

Sie können auch Bereitstellungsprotokolldateien für vCenter Server Appliance erfassen.

- Erfassen von Installationsprotokollen mithilfe des Installationsassistenten auf Seite 274

  Sie können die Seite für unterbrochenes Setup des Installationsassistenten verwenden, um zu der erstellten `.zip`-Datei der Installationsprotokolldateien von vCenter Server für Windows zu gehen.

- Manuelles Abrufen der Installationsprotokolle auf Seite 274

  Sie können die Installationsprotokolldateien zu Prüfzwecken manuell abrufen.

- Erfassen von Bereitstellungsprotokolldateien für die vCenter Server Appliance auf Seite 274

  Wenn die Bereitstellung der vCenter Server Appliance fehlschlägt, können Sie die Protokolldateien laden und in ihnen nach dem Grund des Fehlers suchen.

- Exportieren eines vCenter Server-Support-Pakets zwecks Fehlerbehebung auf Seite 275

  Wenn Sie das Support-Paket der vCenter Server-Instanz in der vCenter Server Appliance zwecks Fehlerbehebung exportieren möchten, können Sie dies über die URL tun, die auf dem DCUI-Startbildschirm angezeigt wird.

Erfassen von Installationsprotokollen mithilfe des Installationsassistenten

Sie können die Seite für unterbrochenes Setup des Installationsassistenten verwenden, um zu der erstellten `.zip`-Datei der Installationsprotokolldateien von vCenter Server für Windows zu gehen.

Wenn die Installation fehlschlägt, wird die Seite zum unterbrochenen Setup angezeigt. Darauf sind die Kontrollkästchen für die Protokollerfassung standardmäßig aktiviert.

Vorgehensweise

1 Lassen Sie die Kontrollkästchen aktiviert und klicken Sie auf **Fertig stellen**.

  Die Installationsdateien werden in einer `ZIP`-Datei auf Ihrem Desktop abgelegt, zum Beispiel `VMware-VCS-logs-`*`Zeitpunkt-des-Installationsversuchs`*`.zip`; dabei steht *Zeitpunkt-des-Installationsversuchs* für das Jahr, den Monat, den Tag, die Stunde, Minuten und Sekunden des Installationsversuchs.

2 Rufen Sie die Protokolldateien aus der `.zip`-Datei auf dem Desktop ab.

Weiter

Prüfen Sie die Protokolldateien, um die Fehlerursache zu ermitteln.

Manuelles Abrufen der Installationsprotokolle

Sie können die Installationsprotokolldateien zu Prüfzwecken manuell abrufen.

Vorgehensweise

1 Navigieren Sie zu den Speicherorten der Installationsprotokolldateien.

  - Verzeichnis `%PROGRAMDATA%\VMware\vCenterServer\logs`, in der Regel `C:\Programme\VMware\vCenterServer\logs`
  - Verzeichnis `%TEMP%`, in der Regel `C:\Users\`*`username`*`\AppData\Local\Temp`

  Zu den Dateien im Verzeichnis `%TEMP%` zählen `vminst.log`, `pkgmgr.log`, `pkgmgr-comp-msi.log` und `vim-vcs-msi.log`.

2 Öffnen Sie die Installationsprotokolldateien in einem Texteditor, um sie zu prüfen.

Erfassen von Bereitstellungsprotokolldateien für die vCenter Server Appliance

Wenn die Bereitstellung der vCenter Server Appliance fehlschlägt, können Sie die Protokolldateien laden und in ihnen nach dem Grund des Fehlers suchen.

Der vollständige Pfad der Protokolldateien wird im Bereitstellungsassistenten der vCenter Server Appliance angezeigt.

Bei einem firstboot-Fehler können Sie das Support-Paket auf einem Windows-Hostsystem herunterladen und in den Protokolldateien ermitteln, welches firstboot-Skript fehlgeschlagen ist. Siehe „Exportieren eines vCenter Server-Support-Pakets zwecks Fehlerbehebung“, auf Seite 275.

Vorgehensweise

1 Wechseln Sie auf dem Windows-System, das Sie zum Bereitstellen der vCenter Server Appliance verwenden, zum Ordner mit den Protokolldateien.

  Wenn Sie als Administrator angemeldet sind, ist dies standardmäßig der Ordner `C:\Users\Administrator\AppData\Local\VMware\CIP\vcsaInstaller`.

2 Öffnen Sie die Installationsprotokolldateien in einem Texteditor, um sie zu prüfen.

Exportieren eines vCenter Server -Support-Pakets zwecks Fehlerbehebung

Wenn Sie das Support-Paket der vCenter Server-Instanz in der vCenter Server Appliance zwecks Fehlerbehebung exportieren möchten, können Sie dies über die URL tun, die auf dem DCUI-Startbildschirm angezeigt wird.

Sie können auch das Supportpaket von der Bash-Shell der vCenter Server Appliance holen, indem Sie das Skript `vc-support.sh` ausführen.

Das Support-Paket wird im `.tgz`-Format exportiert.

Vorgehensweise

1. Melden Sie sich bei der Windows-Hostmaschine an, auf die Sie das Paket herunterladen möchten.
2. Öffnen Sie einen Webbrowser und geben Sie die in der DCUI angezeigte URL des Support-Pakets ein:

   https://*appliance-fully-qualified-domain-name*:443/appliance/support-bundle
3. Geben Sie den Benutzernamen und das Kennwort des Root-Benutzers ein.
4. Drücken Sie die **Eingabetaste**.

   Das Support-Paket wird als `.tgz`-Datei auf Ihre Windows-Maschine heruntergeladen.
5. (Optional) Analysieren Sie die Datei `firstbootStatus.json`, um festzustellen, welches firstboot-Skript fehlgeschlagen ist.

   Wenn Sie das Skript `vc-support.sh` in der Bash-Shell der vCenter Server Appliance ausgeführt haben, führen Sie zum Prüfen der Datei `firstbootStatus.json` folgenden Befehl aus:

   ```
   cat /var/log/firstboot/firstbootStatus.json
   ```

Versuch der Installation eines Platform Services Controller nach einem vorhergehenden Installationsfehler

Wenn Sie Platform Services Controller-Daten replizieren möchten, können Sie möglicherweise nicht einer vCenter Single Sign On-Domäne in einem vorhandenen Platform Services Controller beitreten.

Problem

Wenn Sie versuchen, einen eingebetteten oder externen Platform Services Controller zu installieren, und den Platform Services Controller mit einer vCenter Single Sign On-Domäne oder -Site verbinden, schlägt die Installation möglicherweise fehl, sodass eventuell unvollständige Daten im Platform Services Controller-Verbund verbleiben.

Ursache

Die Platform Services Controller-Daten werden nicht bereinigt, wenn eine Installation eines Platform Services Controller fehlschlägt. Folgendes Szenario wird angenommen:

1. Installieren Sie Platform Services Controller A.
2. Wenn Sie versuchen, Platform Services Controller B zu installieren und mit derselben Domäne wie Platform Services Controller A zu verbinden, schlägt die Installation fehl.
3. Der zweite Versuch, Platform Services Controller B zu installieren und mit derselben Domäne wie Platform Services Controller A zu verbinden, schlägt fehl, weil Platform Services Controller A unvollständige Daten enthält.

Lösung

1. Melden Sie sich als Administrator bei der Maschine an, auf der Sie Platform Services Controller A installieren.

2 Navigieren Sie an der Eingabeaufforderung zum Befehl `vdcleavefed`.

   Der Befehl `vdcleavefed` befindet sich unter Windows im Ordner `C:\Programme\VMware\vCenter Server\vmdird\` und unter Linux im Ordner `/usr/lib/vmware-vmdir/bin/`.

3 Führen Sie den Befehl `vdcleavefed` zum Löschen der Daten aus.

```
vdcleavefed -h Platform-Services-Controller-B-System-Name -u Administrator
```

4 Installieren Sie Platform Services Controller B.

Eine Microsoft SQL-Datenbank, bei der ein nicht unterstützter Kompatibilitätsmodus festgelegt ist, sorgt dafür, dass das Installieren oder das Upgrade von vCenter Server fehlschlägt

Die vCenter Server-Installation mit einer Microsoft SQL-Datenbank schlägt fehl, wenn die Datenbank so eingerichtet ist, dass sie im Kompatibilitätsmodus mit einer nicht unterstützten Version ausgeführt wird.

Problem

Die folgende Fehlermeldung erscheint: `Der eingegebene Datenbankbenutzer verfügt nicht über die erforderlichen Berechtigungen zum Installieren und Konfigurieren von vCenter Server mit der ausgewählten Datenbank. Beheben Sie die folgenden Fehler: %s`

Ursache

vCenter Server muss die Datenbankversion unterstützen. Wenn die Datenbank so eingestellt ist, dass sie im Kompatibilitätsmodus mit einer nicht unterstützten Version ausgeführt wird, tritt dieser Fehler bei SQL auch dann auf, wenn es sich bei der Datenbank um eine unterstützte Version handelt. Wenn beispielsweise SQL 2008 für die Ausführung im SQL 2000-Kompatibilitätsmodus eingestellt ist, tritt dieser Fehler auf.

Lösung

◆ Stellen Sie sicher, dass es sich bei der vCenter Server-Datenbank um eine unterstützte Version handelt und sie nicht so eingerichtet ist, dass sie im Kompatibilitätsmodus mit einer nicht unterstützten Version ausgeführt wird. Siehe die VMware-Produkt-Interoperabilitätsmatrix unter http://partnerweb.vmware.com/comp_guide2/sim/interop_matrix.php?.

Nach der Installation des vCenter Server oder der Bereitstellung der vCenter Server Appliance

11

Nachdem Sie den vCenter Server installiert oder die vCenter Server Appliance bereitgestellt haben, erwägen Sie die folgenden Post-Installationsoptionen, bevor Sie dem vCenter Server Bestand zur Verwaltung hinzufügen.

Dieses Kapitel behandelt die folgenden Themen:

Anmelden bei vCenter Server mithilfe von vSphere Web Client

Melden Sie sich über vCenter Server bei vSphere Web Client an, um die vSphere-Bestandsliste zu verwalten.

Voraussetzungen

Wenn Sie vCenter Server 5.0 mit dem vSphere Web Client einsetzen möchten, überprüfen Sie, ob das vCenter Server 5.0-System beim vSphere Web Client registriert ist.

Wenn Sie vCenter Server 5.1 oder vCenter Server 5.5 mit dem vSphere Web Client verwenden möchten, überprüfen Sie, ob vCenter Server installiert ist und sowohl vCenter Server als auch der vSphere Web Client auf dieselbe vCenter Single Sign-On-Instanz verweisen.

In vSphere 6.0 wird der vSphere Web Client im Rahmen der Bereitstellung von vCenter Server unter Windows oder der Bereitstellung von vCenter Server Appliance installiert. Auf diese Weise verweist der vSphere Web Client stets auf dieselbe vCenter Single Sign-On-Instanz.

Vorgehensweise

1. Öffnen Sie einen Webbrowser und geben Sie die URL für den vSphere Web Client ein: **https://*client-hostname*/vsphere-client**.
2. Geben Sie die Anmeldedaten eines Benutzers mit Berechtigungen für vCenter Server ein und klicken Sie auf **Anmelden**.

3 Wenn eine Warnmeldung zu einem nicht vertrauenswürdigen SSL-Zertifikat angezeigt wird, wählen Sie basierend auf Ihrer Sicherheitsrichtlinie die entsprechende Aktion aus.

Option	Aktion
Ignorieren Sie die Sicherheitswarnung nur für diese Anmeldesitzung.	Klicken Sie auf **Ignorieren**.
Ignorieren Sie die Sicherheitswarnung für diese Anmeldesitzung und installieren Sie das Standardzertifikat, damit die Warnung nicht erneut angezeigt wird.	Wählen Sie **Dieses Zertifikat installieren und keine Sicherheitswarnungen für diesen Server anzeigen** und klicken Sie auf **Ignorieren**. Wählen Sie diese Option nur, wenn das Standardzertifikat verwendet werden kann, ohne dass es in Ihrer Umgebung ein Sicherheitsproblem darstellt.
Klicken Sie auf „Abbrechen“ und installieren Sie ein signiertes Zertifikat, bevor Sie fortfahren.	Klicken Sie auf **Abbrechen** und stellen Sie sicher, dass ein signiertes Zertifikat auf dem vCenter Server-System installiert ist, bevor Sie erneut versuchen, die Verbindung herzustellen.

Der vSphere Web Client stellt eine Verbindung zu allen vCenter Server-Systemen her, für die der Benutzer Berechtigungen hat, sodass Sie die Bestandsliste anzeigen und verwalten können.

Erfassen von vCenter Server -Protokolldateien

Nach der Installation von vCenter Server können Sie die vCenter Server-Protokolldateien zur Diagnose und Fehlerbehebung erfassen.

Hinweis In diesem Thema erfahren Sie, wie Sie die Protokolldateien für eine Windows-Installation von vCenter Server erfassen. Informationen zum Exportieren eines Support-Pakets und zum Durchsuchen der Protokolldateien in der vCenter Server Appliance finden Sie unter *vCenter Server Appliance-Konfiguration*.

Vorgehensweise

1 Melden Sie sich als Administrator bei dem Windows-System an, auf dem vCenter Server installiert ist.

2 Generieren Sie das Protokollpaket.

- Klicken Sie auf **Start > Programme > VMware > vCenter Server-Protokollpaket generieren**.

  Sie können auch dann vCenter Server-Protokollpakete generieren, wenn Sie mit dem vSphere Web Client keine Verbindung zu vCenter Server herstellen können.

- Wechseln Sie in der Eingabeaufforderung zu `*Installationsverzeichnis*\VMware\vCenter Server\bin` und führen Sie den Befehl `vc-support.bat` aus.

Die Protokolldateien für das vCenter Server-System werden generiert und in einem `TGZ`-Archiv auf Ihrem Desktop gespeichert.

Installieren oder Durchführen eines Upgrades von vSphere Authentication Proxy

Installieren Sie vSphere Authentication Proxy, um ESXi-Hosts den Beitritt zu einer Domäne zu ermöglichen, ohne Active Directory-Anmeldeinformationen zu verwenden. vSphere Authentication Proxy verbessert die Sicherheit für von PXE gestartete Hosts sowie von Hosts, die unter Verwendung von Auto Deploy bereitgestellt werden, weil Active Directory-Anmeldeinformationen nicht in der Hostkonfiguration gespeichert werden müssen.

Wenn auf Ihrem System eine frühere Version von vSphere Authentication Proxy installiert ist, sorgt dieser Vorgang dafür, dass ein Upgrade von vSphere Authentication Proxy auf die aktuelle Version durchgeführt wird.

Sie können vSphere Authentication Proxy auf derselben Maschine wie den verknüpften vCenter Server oder auf einer anderen Maschine installieren, die über eine Netzwerkverbindung mit vCenter Server verfügt. vSphere Authentication Proxy wird ab vCenter Server-Version 5.0 unterstützt.

Der vSphere Authentication Proxy-Dienst bindet an eine IPv4-Adresse für die Kommunikation mit vCenter Server und bietet keine Unterstützung für IPv6. Die vCenter Server-Instanz kann sich auf einer Hostmaschine in einer Netzwerkumgebung befinden, in der nur IPv4, IPv4 und IPv6 oder nur IPv6 eingesetzt wird. Allerdings muss die Maschine, die eine Verbindung zu vCenter Server über den vSphere Web Client herstellt, über eine IPv4-Adresse verfügen, damit der vSphere Authentication Proxy-Dienst funktionieren kann.

Voraussetzungen

- Installieren Sie Microsoft .NET Framework 3.5 auf dem System, auf dem Sie vSphere Authentication Proxy installieren möchten.
- Stellen Sie sicher, dass Sie über Administratorberechtigungen verfügen.
- Stellen Sie sicher, dass die Hostmaschine über einen unterstützten Prozessor und ein unterstütztes Betriebssystem verfügt.
- Achten Sie darauf, dass die Hostmaschine über eine gültige IPv4-Adresse verfügt. Sie können vSphere Authentication Proxy auf einer Maschine in einer Netzwerkumgebung installieren, in der nur IPv4 oder sowohl IPv4 als auch IPv6 eingesetzt werden. Sie können vSphere Authentication Proxy jedoch nicht in einer Netzwerkumgebung installieren, in der nur IPv6 eingesetzt wird.
- Wenn Sie vSphere Authentication Proxy auf einer Windows Server 2008 R2-Hostmaschine installieren, laden Sie den im Windows-KB-Artikel 981506 auf der Website support.microsoft.com beschriebenen Windows-Hotfix herunter und installieren Sie ihn. Wenn dieser Hotfix nicht installiert ist, kann der vSphere Authentication Proxy-Adapter nicht initialisiert werden. Zu diesem Problem werden Fehlermeldungen in der Datei `camadapter.log` protokolliert, die den Meldungen `CAM–Website konnte nicht mit CTL gebunden werden` und `CAMAdapter konnte nicht initialisiert werden` ähneln.
- Laden Sie das vCenter Server-Installationsprogramm herunter.

Sammeln Sie die folgenden Informationen, um die Installation bzw. das Upgrade abzuschließen:

- Der Installationsspeicherort von vSphere Authentication Proxy, wenn Sie den Standardspeicherort nicht verwenden.
- Die Adresse und Anmeldeinformationen von vCenter Server, mit dem vSphere Authentication Proxy eine Verbindung herstellt: IP-Adresse oder Name, HTTP-Port, Benutzername und Kennwort.
- Der Hostname oder die IP-Adresse, die zum Identifizieren von vSphere Authentication Proxy im Netzwerk verwendet wird.

Vorgehensweise

1. Fügen Sie die Hostmaschine dort hinzu, wo Sie den Authentication Proxy-Dienst für die Domäne installieren.
2. Verwenden Sie das Domänenadministratorkonto, um sich bei der Hostmaschine anzumelden.
3. Doppelklicken Sie im Software-Installationsprogrammverzeichnis auf die Datei `autorun.exe`, um das Installationsprogramm zu starten.
4. Wählen Sie **VMware vSphere Authentication Proxy** aus und klicken Sie auf **Installieren**.
5. Folgen Sie den Eingabeaufforderungen des Assistenten, um die Installation bzw. das Upgrade abzuschließen.

   Während der Installation registriert sich der Authentifizierungsdienst mit der vCenter Server-Instanz, auf der Auto Deploy registriert ist.

Wenn Sie den vSphere Authentication Proxy-Dienst installieren, erstellt das Installationsprogramm ein Domänenkonto mit den entsprechenden Berechtigungen zum Ausführen des Authentication Proxy-Diensts. Der Name des Kontos beginnt mit dem Präfix `CAM–` und ihm wird ein 32-stelliges, nach dem Zufallsprinzip generiertes Kennwort zugeordnet. Das Kennwort ist so konfiguriert, dass es nie abläuft. Ändern Sie die Kontoeinstellungen nicht.

Weiter

Konfigurieren Sie ESXi für die Verwendung von vSphere Authentication Proxy zum Beitritt in eine Domäne. Informationen finden Sie in der Dokumentation *vSphere-Sicherheit*.

Deinstallieren von vCenter Server

Sie müssen über Administratorberechtigungen verfügen, um VMware vCenter Server deinstallieren zu können.

WICHTIG Wenn Sie die eingebettete PostgreSQL-Datenbank verwenden, wird bei der Deinstallation von vCenter Server auch die eingebettete Datenbank deinstalliert, und alle Daten gehen verloren.

Voraussetzungen

Wenn Sie das vCenter Server-System deinstallieren, entfernen Sie die Hosts aus der Host- und Clusterbestandsliste.

Vorgehensweise

1. Klicken Sie als Administratorbenutzer im Windows-System auf **Start > Systemsteuerung > Programme und Funktionen**.
2. Wählen Sie **VMware vCenter Server** aus der Liste aus und klicken Sie auf **Entfernen**.
3. Klicken Sie auf **Entfernen**, um das Entfernen des Programms zu bestätigen.
4. Klicken Sie auf **Beenden**.

Neuverweisen der Verbindungen zwischen vCenter Server und Platform Services Controller

Durch Verbinden externer Platform Services Controller-Instanzen in derselben vCenter Single Sign-On-Domäne wird die Hochverfügbarkeit Ihres Systems sichergestellt.

Wenn Ihre Umgebung externe Platform Services Controller-Instanzen enthält, die die Infrastrukturdaten in einer einzelnen Domäne replizieren, können Sie die vCenter Server-Instanzen zu einem anderen Platform Services Controller umleiten. Wenn ein externer Platform Services Controller nicht mehr antwortet, können Sie die vCenter Server-Instanzen neu auf einen anderen Platform Services Controller in derselben Domäne verweisen.

Wenn Sie die Last einer externen Platform Services Controller-Instanz verteilen möchten, können Sie einige vCenter Server-Instanzen neu auf andere Platform Services Controller-Instanzen in derselben Domäne verweisen.

Voraussetzungen

Stellen Sie sicher, dass die externen Platform Services Controller-Instanzen die Infrastrukturdaten in einer einzelnen Domäne replizieren.

Vorgehensweise

1 Melden Sie sich bei der vCenter Server-Instanz an.

- Melden Sie sich für vCenter Server Appliance bei der vCenter Server Appliance-Shell als **root** an.
- Melden Sie sich für eine unter Windows installierte vCenter Server-Instanz als Administrator bei der virtuellen Maschine oder beim physischen Server an, auf der bzw. dem Sie vCenter Server installiert haben.

2 Führen Sie das Skript `cmsso-util` aus.

```
cmsso-util repoint --repoint-psc psc_fqdn_or_static_ip [--dc-port port_number]
```

wobei die rechteckigen Klammern die Befehlsoptionen einschließen.

Dabei ist *psc_fqdn_or_static_ip* der Systemname, mit dem der Platform Services Controller identifiziert wird. Dieser Systemname muss ein FQDN oder eine statische IP-Adresse sein.

Verwenden Sie die Option `--dc-port port_number`, falls der Platform Services Controller auf einem benutzerdefinierten HTTPS-Port ausgeführt wird. Der Standardwert für den HTTPS-Port ist 443.

3 Melden Sie sich mit dem vSphere Web Client bei der vCenter Server-Instanz an und prüfen Sie, ob der vCenter Server ausgeführt wird und verwaltet werden kann.

Die vCenter Server-Instanz wird mit dem neuen Platform Services Controller registriert.

Neukonfigurieren von vCenter Server mit eingebettetem Platform Services Controller als vCenter Server mit externem Platform Services Controller

Wenn Sie vCenter Server mit eingebettetem Platform Services Controller installieren, können Sie diese Instanz in einen vCenter Server konvertieren und auf einen externen Platform Services Controller innerhalb derselben Domäne neu verweisen.

WICHTIG Sie können Snapshots von vCenter Server mit eingebettetem Platform Services Controller und dem externen Platform Services Controller erstellen, damit Sie die Snapshots wiederherstellen können, falls die Neukonfiguration fehlschlägt.

Voraussetzungen

- Stellen Sie sicher, dass nur ein externer Platform Services Controller installiert ist.
- Stellen Sie sicher, dass sich der externe Platform Services Controller in derselben vCenter Single Sign-On-Domäne wie der eingebettete Platform Services Controller befindet.

Vorgehensweise

1 Melden Sie sich bei der vCenter Server-Instanz an.

- Melden Sie sich für vCenter Server Appliance bei der vCenter Server Appliance-Shell als **root** an.
- Melden Sie sich für eine unter Windows installierte vCenter Server-Instanz als Administrator bei der virtuellen Maschine oder beim physischen Server an, auf der bzw. dem Sie vCenter Server installiert haben.

2 Stellen Sie sicher, dass alle Platform Services Controller-Dienste der eingebetteten Platform Services Controller-Instanz ausgeführt werden.

   Die folgenden Platform Services Controller-Dienste müssen ausgeführt werden: VMware-Lizenzdienst, VMware Identity Management-Dienst, VMware Security Token-Dienst, VMware-Zertifikatdienst und VMware-Verzeichnisdienst.

   - Für einen als Appliance bereitgestellten Platform Services Controller führen Sie den Befehl `service-control --status --all` aus.
   - Für einen unter Windows installierten Platform Services Controller wählen Sie im **Start**-Menü von Windows **Systemsteuerung > Verwaltung > Dienste** aus.

3 Führen Sie das Skript `cmsso-util` aus.

```
cmsso-util reconfigure --repoint-psc psc_fqdn_or_static_ip --username username --domain-name
domain_name --passwd password [--dc-port port_number]
```

   wobei die eckigen Klammern [ ] optionale Elemente einschließen.

   Dabei ist *psc_fqdn_or_static_ip* der Systemname, mit dem der Platform Services Controller identifiziert wird. Dieser Systemname muss ein FQDN oder eine statische IP-Adresse sein. Die Optionen *username* und *password* sind der Benutzername und das Kennwort des Administrators für vCenter Single Sign-On *domain_name*. Verwenden Sie die Option `--dc-port`, falls der externe Platform Services Controller auf einem benutzerdefinierten HTTPS-Port ausgeführt wird. Der Standardwert für den HTTPS-Port ist 443.

   Wenn beispielsweise der externe Platform Services Controller auf dem benutzerdefinierten HTTPS-Port 449 ausgeführt wird, müssen Sie folgenden Befehl ausführen:

```
cmsso-util reconfigure --repoint-psc psc.acme.local --username administrator --domain-name
vsphere.local --passwd Password1! --dc-port 449
```

4 Melden Sie sich mit dem vSphere Web Client bei der vCenter Server-Instanz an und prüfen Sie, ob der vCenter Server ausgeführt wird und verwaltet werden kann.

Der vCenter Server mit eingebettetem Platform Services Controller wird herabgestuft, und der vCenter Server wird an den externen Platform Services Controller umgeleitet.

Sichern und Wiederherstellen einer vCenter Server -Umgebung 12

Sie können vSphere Data Protection zum Sichern und Wiederherstellen einer virtuellen Maschine (VM) verwenden, die vCenter Server, eine vCenter Server Appliance oder einen Platform Services Controller enthält.

vSphere Data Protection ist eine durch EMC betriebene und auf Datenträgern basierte Lösung zum Sichern und Wiederherstellen. vSphere Data Protection ist vollkommen auf vCenter Server abgestimmt und Sie können damit Sicherungsaufgaben verwalten, während Sicherungen an deduplizierten Zielspeicherorten gespeichert werden. Nach dem Bereitstellen und Konfigurieren von vSphere Data Protection können Sie über die Benutzeroberfläche von vSphere Web Client zum Auswählen, Planen, Konfigurieren und Verwalten von Sicherungen und Wiederherstellungen von virtuellen Maschinen auf vSphere Data Protection zugreifen. Bei der Sicherung erstellt vSphere Data Protection einen Snapshot der stillgelegten virtuellen Maschine. Die Deduplizierung wird bei jedem Sicherungsvorgang automatisch durchgeführt.

In vSphere 6.0 müssen Sie zum Sichern und Wiederherstellen einer virtuellen Maschine, die vCenter Server, eine vCenter Server Appliance oder einen Platform Services Controller enthält, eine vollständige Image-Sicherung durchführen und die virtuelle Maschine muss die folgenden Voraussetzungen erfüllen:

- Auf der virtuellen Maschinen muss VMware Tools installiert sein und ausgeführt werden.
- Die virtuelle Maschine muss einen vollqualifizierten Domänennamen (FQDN) mit korrekter DNS-Auflösung verwenden oder muss mit einer statischen IP-Adresse konfiguriert sein.

Die folgenden Sicherungen und Wiederherstellungen werden nicht unterstützt:

- Inkrementelle Sicherungen
- Differenzielle Sicherungen
- Sicherungen einzelner Datenträger
- Virtuelle Maschinen mit Snapshots
- Virtuelle Maschinen mit konfigurierter Fault Tolerance

Sie können außerdem mit vSphere Data Protection eine virtuelle Maschine, die eine vCenter Server- oder Platform Services Controller-Instanz enthält, direkt auf dem ESXi-Host, der die vSphere Data Protection-Appliance ausführt, wiederherstellen, wenn der vCenter Server-Dienst nicht verfügbar ist oder wenn Sie nicht über den vSphere Web Client auf die Benutzeroberfläche von vSphere Data Protection zugreifen können.

Im Abschnitt „Allgemeiner Workflow für vSphere Data Protection", auf Seite 284 finden Sie Informationen zu grundlegenden vSphere Data Protection-Aufgaben. In den Abschnitten „Sichern und Wiederherstellen von vCenter Server mit eingebettetem Platform Services Controller", auf Seite 292, „Sichern und Wiederherstellen einer vCenter Server-Umgebung mit einem einzelnen externen Platform Services Controller",

auf Seite 293 und „Sichern und Wiederherstellen einer vCenter Server-Umgebung mit mehreren Platform Services Controller-Instanzen", auf Seite 295 finden Sie detaillierte Workflows zum Sichern und Wiederherstellen Ihrer Umgebung in Abhängigkeit vom Bereitstellungstyp und der Anzahl von Platform Services Controller-Instanzen.

Dieses Kapitel behandelt die folgenden Themen:

Allgemeiner Workflow für vSphere Data Protection

Zum Sichern und Wiederherstellen einer virtuellen Maschine, die vCenter Server, eine vCenter Server Appliance oder einen Platform Services Controller enthält, müssen Sie vSphere Data Protection bereitstellen und konfigurieren und grundlegende Sicherungs- und Wiederherstellungsaufgaben ausführen.

Bereitstellen der OVF-Vorlage für vSphere Data Protection

Stellen Sie vSphere Data Protection zum Sichern und Wiederherstellen einer virtuellen Maschine bereit, die vCenter Server oder die vCenter Server Appliance enthält.

Voraussetzungen

- Stellen Sie sicher, dass Sie ESXi 5.0 oder höher verwenden.
- Wenn in Ihrer Umgebung eine Firewall aktiviert ist, stellen Sie sicher, dass Port 902 für den Datenaustausch zwischen der vSphere Data Protection-Appliance und dem ESXi-Host geöffnet ist. Weitere Informationen finden Sie in der Dokumentation für *vSphere Data Protection*.
- Stellen Sie sicher, dass das VMware Client-Integrations-Plug-In für Ihren Browser installiert ist. Weitere Informationen finden Sie unter „Installieren des Client-Integrations-Plug-Ins", auf Seite 261.
- Verwenden Sie den vSphere Web Client zum Anmelden als Administrator bei der vCenter Server-Instanz, die Ihre Umgebung verwaltet.

Vorgehensweise

1. Wählen Sie **vCenter > Datencenter** aus.
2. Klicken Sie auf der Registerkarte **Objekte** auf **Aktionen** und wählen Sie **OVF-Vorlage bereitstellen** aus.
3. Navigieren Sie zu der OVA-Datei der vSphere Data Protection-Appliance und klicken Sie auf **Öffnen**.
4. Überprüfen Sie die OVF-Vorlagendetails und klicken Sie auf **Weiter**.
5. Überprüfen Sie die Vorlagendetails, klicken Sie auf **Weiter** und führen Sie die angezeigten Anweisungen des Assistenten zum Akzeptieren der Lizenzvereinbarung aus.

6 Geben Sie auf der Seite „Namen und Ordner auswählen“ einen vollständig qualifizierten Domänennamen (FQDN) für die vSphere Data Protection-Appliance ein, wählen Sie den Ordner oder das Datencenter, in dem Sie die vSphere Data Protection-Appliance bereitstellen möchten, aus und klicken Sie auf **Weiter**.

   Die vSphere Data Protection-Konfiguration verwendet den Namen, den Sie eingeben, um die vSphere Data Protection-Appliance in der vCenter Server-Bestandsliste zu finden. Ändern Sie nicht den Namen der vSphere Data Protection-Appliance nach der Installation.

7 Wählen Sie den Host aus, auf dem die vSphere Data Protection-Appliance bereitgestellt werden soll, und klicken Sie auf **Weiter**.

8 Wählen Sie das Format der virtuellen Festplatte und den Speicherort für die vSphere Data Protection-Appliance aus und klicken Sie auf **Weiter**.

9 Wählen Sie das Zielnetzwerk für die vSphere Data Protection-Appliance aus und klicken Sie auf **Weiter**.

10 Geben Sie auf der Seite „Vorlage anpassen“ die Netzwerkeinstellungen wie beispielsweise Standard-Gateway, DNS, Netzwerk-IP-Adresse und Netzmaske ein und klicken Sie auf **Weiter**.

   Prüfen Sie, ob die IP-Adressen korrekt sind und mit dem Eintrag im DNS-Server übereinstimmen. Wenn Sie falsche IP-Adressen eingeben, müssen Sie die vSphere Data Protection-Appliance neu bereitstellen.

   HINWEIS Die vSphere Data Protection-Appliance unterstützt DHCP nicht. Eine statische IP-Adresse ist erforderlich.

11 Prüfen Sie auf der Seite „Bereit zum Abschließen“, ob alle Bereitstellungsoptionen korrekt sind, wählen Sie **Nach der Bereitstellung einschalten** aus und klicken Sie auf **Beenden**.

Der Bereitstellungsvorgang für die vSphere Data Protection-Appliance wird gestartet und die vSphere Data Protection-Appliance startet im Installationsmodus.

Weiter

Konfigurieren Sie die Anfangseinstellungen von vSphere Data Protection. Siehe „Konfigurieren von vSphere Data Protection“, auf Seite 285.

Konfigurieren von vSphere Data Protection

Bei der Erstkonfiguration von vSphere Data Protection können Sie die Netzwerkeinstellungen und Zeitzonendaten für Ihre vSphere Data Protection-Appliance festlegen. Sie verwenden den Assistenten zur Konfiguration von vSphere Data Protection zum Registrieren der vSphere Data Protection-Appliance bei vCenter Server.

Voraussetzungen

- Stellen Sie die vSphere Data Protection-Appliance bereit.
- Lesen Sie im *vSphere Data Protection-Administratorhandbuch* die komplette Liste der Schritte zum Konfigurieren von vSphere Data Protection.
- Prüfen Sie, ob im Datenspeicher genug Festplattenspeicherplatz verfügbar ist. Wenn bei der Erstkonfiguration der Appliance ein optionaler Leistungsanalysetest ausgeführt wird, werden auf jedem Datenspeicher für jede Festplatte 41 GB benötigt. Wenn der verfügbare Speicherplatz nicht ausreicht, werden bei der Analyse der Wert 0 für alle Lese-, Schreib- und Suchtests und der endgültige Status „Nicht genug Speicherplatz“ angezeigt.
- Verwenden Sie den vSphere Web Client zum Anmelden als Administrator bei der vCenter Server-Instanz, die Ihre Umgebung verwaltet.

Vorgehensweise

1. Wählen Sie im vSphere Web Client die Option **vCenter-Bestandslisten > Virtuelle Maschinen** aus.
2. Klicken Sie mit der rechten Maustaste auf die vSphere Data Protection-Appliance und wählen Sie **Konsole öffnen** aus.

   Nach dem Laden der Installationsdateien wird der Bildschirm „Willkommen" für das Menü von vSphere Data Protection eingeblendet.
3. Navigieren Sie in einem Webbrowser zur URL des Konfigurationsdienstprogramms von vSphere Data Protection.

   https://*ip_address_VDP_Appliance*:8543/vdp-configure/
4. Melden Sie sich als Root an.

   Das Standardkennwort lautet „changeme".

   Der Assistent für die vSphere Data Protection-Konfiguration wird eingeblendet.
5. Geben Sie auf der Assistentenseite mit den Netzwerkeinstellungen die Netzwerk- und Serverdaten für die vSphere Data Protection-Appliance ein bzw. prüfen Sie sie und klicken Sie auf **Weiter**.

   Stellen Sie sicher, dass die richtigen Werte eingetragen sind, andernfalls schlägt die Erstkonfiguration fehl.
6. Wählen Sie die entsprechende Zeitzone für die vSphere Data Protection-Appliance aus und klicken Sie auf **Weiter**.
7. Wählen Sie auf der Seite für die VDP-Anmeldedaten ein neues Root-Kennwort für die virtuelle Appliance aus und klicken Sie auf **Weiter**.
8. Registrieren Sie auf der Seite „vCenter-Registrierung" die Appliance bei vCenter Server:

   a. Geben Sie im Textfeld **vCenter-Benutzername** einen Benutzernamen für vCenter Server ein.

      Wenn der Benutzer zu einem Domänenkonto gehört, geben Sie den Benutzernamen im Format *DOMÄNE\Benutzername* ein.

      WICHTIG Wenn Sie den vCenter Single Sign On-Administratorbenutzernamen im UPN (Benutzerprinzipalname)-Format eingeben, werden die mit vSphere Data Protection-Vorgängen verknüpften Aufgaben nicht im Bereich „Kürzlich bearbeitete Aufgaben" von vSphere Web Client angezeigt. Wenn Sie den vCenter Single Sign On-Administratorbenutzernamen verwenden möchten, geben Sie den Benutzernamen für vCenter Single Sign On im UPN-Format ein.

      ---

   b. Geben Sie im Textfeld **vCenter-Kennwort** das vCenter Server-Kennwort ein.

   c. Geben Sie einen vCenter-FQDN oder eine IP-Adresse ein.

   d. Ändern Sie den Standard-HTTP-Port für vCenter Server.

      Geben Sie einen benutzerdefinierten Wert für den HTTP-Port ein, wenn Sie sich mit vCenter Server über den HTTP-Port anstelle des HTTPS-Ports verbinden müssen, der für den anderen Datenaustausch verwendet wird.

   e. Geben Sie einen vCenter-HTTPS-Port ein (443 ist der Standardport).

   f. Aktivieren Sie das Kontrollkästchen **vCenter für SSO-Authentifizierung verwenden**.

   g. (Optional) Klicken Sie auf **Testverbindung**.

      Eine Meldung zum Verbindungserfolg wird angezeigt. Wenn diese Meldung nicht angezeigt wird, suchen Sie nach Fehlern bei Ihren Einstellungen und wiederholen Sie diesen Schritt, bis eine Erfolgsmeldung eingeblendet wird.

9 Klicken Sie auf **Weiter** und befolgen Sie die Anweisungen des Assistenten, um die Konfiguration fertigzustellen.

Weiter

Erstellen Sie eine Sicherungsaufgabe mit einer bestimmten Aufbewahrungsrichtlinie und einem Sicherungsplan. Weitere Informationen finden Sie unter „Erstellen einer Sicherungsaufgabe in vSphere Data Protection“, auf Seite 287.

Erstellen einer Sicherungsaufgabe in vSphere Data Protection

Sie können Sicherungsaufgaben erstellen, um die Sicherung eines Satzes von einer oder mehreren virtuellen Maschinen, die vCenter Server, die vCenter Server Appliance und Platform Services Controller enthalten, mit einem Sicherungsplan und bestimmten Aufbewahrungsrichtlinien zu verknüpfen.

Voraussetzungen

- Stellen Sie die vSphere Data Protection-Appliance bereit und konfigurieren Sie sie.
- Verwenden Sie den vSphere Web Client zum Anmelden bei der vCenter Server-Instanz, die Ihre Umgebung verwaltet. Melden Sie sich als der Benutzer mit Administratorrechten an, der während der Konfiguration von vSphere Data Protection verwendet wurde.

Vorgehensweise

1 Klicken Sie auf der Startseite von vSphere Web Client auf **vSphere Data Protection**.

2 Wählen Sie im Menü **Aktionen der Sicherungsaufgabe** die Option **Neu** zum Ausführen des Assistenten Neue Sicherungsaufgabe erstellen aus.

3 Wählen Sie auf der Seite „Auftragstyp“ die Option **Gast-Images** aus und klicken Sie auf **Weiter**.

4 Wählen Sie auf der Seite „Datentyp“ die Option **Vollbild** aus und klicken Sie auf **Weiter**.

Sie können alle Objekte und virtuellen Maschinen in der vCenter Server-Bestandsliste sehen.

5 Wählen Sie auf der Seite für Sicherungsziele die virtuelle Maschine aus, die die zu sichernde vCenter Server- oder Platform Services Controller-Instanz enthält, und klicken Sie auf **Weiter**.

6 Wählen Sie auf der Seite „Zeitplan“ den Zeitplan für die Sicherungsaufgabe aus und klicken Sie auf **Weiter**.

7 Wählen Sie auf der Seite „Aufbewahrungsrichtlinie“ einen Aufbewahrungszeitraum aus und klicken Sie auf **Weiter**.

Hinweis Wenn Sie einen neuen Wartungszeitraum eingeben, der dem Ablauf einer Sicherung folgt, entfernt die vSphere Data Protection-Appliance ihren Verweis auf die Sicherungsdaten und Sie können die abgelaufene Sicherung nicht wiederherstellen. Die vSphere Data Protection-Appliance ermittelt, ob die Sicherungsdaten von einem anderen Wiederherstellungspunkt verwendet werden. Wenn die Daten nicht verwendet werden, werden sie entfernt und Festplattenkapazität wird verfügbar.

---

8 Geben Sie auf der Seite „Name“ einen Namen für die Sicherungsaufgabe ein und klicken Sie auf **Weiter**.

9 Überprüfen Sie auf der Seite „Bereit zum Abschließen“ die zusammengefassten Informationen für die Sicherungsaufgabe und klicken Sie auf **Beenden**.

Die neu erstellte Sicherungsaufgabe wird auf der Registerkarte **Sicherung** aufgeführt. Die Sicherungsaufgabe wird automatisch gemäß dem konfigurierten Zeitplan gestartet.

Weiter

- Vorhandene Sicherungsaufgabe sofort ausführen. Weitere Informationen finden Sie unter „Erstellen einer Sicherungsaufgabe in vSphere Data Protection“, auf Seite 287.

- Stellen Sie eine gesicherte vCenter Server-, vCenter Server Appliance- oder Platform Services Controller-Instanz wieder her. Weitere Informationen finden Sie unter „Wiederherstellen einer vCenter Server-Umgebung“, auf Seite 288.

Manuelles Starten einer Sicherungsaufgabe

Eine Sicherung wird entsprechend dem in der Sicherungsaufgabe konfigurierten geplanten Datum und Zeitpunkt sowie der konfigurierten Häufigkeit automatisch gestartet. Wenn Sie eine vorhandene Sicherungsaufgabe sofort ausführen möchten, können Sie den Vorgang manuell starten.

Voraussetzungen

- Stellen Sie die vSphere Data Protection-Appliance bereit und konfigurieren Sie sie.
- Erstellen Sie eine Sicherungsaufgabe. Siehe „Erstellen einer Sicherungsaufgabe in vSphere Data Protection“, auf Seite 287.
- Verwenden Sie den vSphere Web Client zum Anmelden bei der vCenter Server-Instanz, die Ihre Umgebung verwaltet. Melden Sie sich als der Benutzer mit Administratorrechten an, der während der Konfiguration von vSphere Data Protection verwendet wurde.

Vorgehensweise

1. Klicken Sie auf der Startseite von vSphere Web Client auf **vSphere Data Protection**.
2. Wählen Sie auf der Registerkarte **Sicherung** die auszuführende Sicherungsaufgabe aus.
3. Klicken Sie auf **Jetzt sichern** und wählen Sie **Alle Quellen sichern** aus.

   In einem Dialogfeld wird bestätigt, dass die Sicherung erfolgreich initiiert wurde.

Weiter

Stellen Sie eine gesicherte vCenter Server-, vCenter Server Appliance- oder Platform Services Controller-Instanz wieder her. Weitere Informationen finden Sie unter „Wiederherstellen einer vCenter Server-Umgebung“, auf Seite 288.

Wiederherstellen einer vCenter Server -Umgebung

Nach dem Sichern einer virtuellen Maschine, die vCenter Server, vCenter Server Appliance oder Platform Services Controller enthält, können Sie die Sicherungs-Images am ursprünglichen Speicherort oder an einem neuen Speicherort wiederherstellen.

Sie können virtuelle Maschinen am ursprünglichen Speicherort wiederherstellen, indem Sie entweder die gesicherte virtuelle Maschine überschreiben oder eine neue virtuelle Maschine erstellen, die die wiederhergestellte vCenter Server-, vCenter Server Appliance- oder Platform Services Controller-Instanz auf demselben ESXi-Host enthält. Sie können auch die virtuelle Maschine auf einem neuen ESXi-Host wiederherstellen.

Wichtig Die Wiederherstellung von VMs, die Snapshots aufweisen, wird nicht unterstützt.

Sie können eine virtuelle Maschine auf dem ESXi-Host wiederherstellen, auf dem die vSphere Data Protection-Appliance ausgeführt wird. Mit der Direct-to-Host-Notfallwiederherstellung können Sie eine virtuelle Maschine wiederherstellen, wenn der vCenter Server nicht mehr verfügbar ist oder wenn der Benutzer nicht über den vSphere Web Client auf die Benutzeroberfläche von vSphere Data Protection zugreifen kann.

-

  Sie können vollständige Image-Sicherungen von virtuellen Maschinen, die vCenter Server, vCenter Server Appliance oder Platform Services Controller enthalten, mit dem Assistenten zum Wiederherstellen von Sicherungen manuell wiederherstellen.

- Wiederherstellen einer virtuellen Maschine an einem neuen Speicherort auf Seite 290

  Sie können vollständige Image-Sicherungen manuell mit dem Assistenten zum Wiederherstellen von Sicherungen wiederherstellen.

- Wiederherstellen einer virtuellen Maschine mit der Direct-to-Host-Notfallwiederherstellung auf Seite 291

  Mit der Direct-to-Host-Notfallwiederherstellung können Sie die virtuelle Maschine wiederherstellen, die vCenter Server, vCenter Server Appliance oder Platform Services Controller enthält, wenn vCenter Server nicht mehr verfügbar ist oder wenn Sie nicht über den vSphere Web Client auf die Benutzeroberfläche von vSphere Data Protection zugreifen können.

Wiederherstellen einer virtuellen Maschine am ursprünglichen Speicherort

Sie können vollständige Image-Sicherungen von virtuellen Maschinen, die vCenter Server, vCenter Server Appliance oder Platform Services Controller enthalten, mit dem Assistenten zum Wiederherstellen von Sicherungen manuell wiederherstellen.

Voraussetzungen

- Stellen Sie die vSphere Data Protection-Appliance bereit und konfigurieren Sie sie.
- Sichern Sie eine virtuelle Maschine, auf der vCenter Server, vCenter Server Appliance oder Platform Services Controller ausgeführt wird. Siehe „Erstellen einer Sicherungsaufgabe in vSphere Data Protection“, auf Seite 287.
- Verwenden Sie den vSphere Web Client zum Anmelden bei der vCenter Server-Instanz, die Ihre Umgebung verwaltet. Melden Sie sich als der Benutzer mit Administratorrechten an, der während der Konfiguration von vSphere Data Protection verwendet wurde.
- Stellen Sie sicher, dass die virtuelle Maschine, die Sie wiederherstellen möchten, ausgeschaltet ist.

Vorgehensweise

1. Klicken Sie auf der Startseite von vSphere Web Client auf **vSphere Data Protection**.
2. Klicken Sie auf die Registerkarte **Wiederherstellen**.
3. (Optional) Filtern Sie die Sicherungen zum Verfeinern Ihrer Suche.
4. Wählen Sie eine virtuelle Maschine in der Spalte „Name“ und dann mindestens ein Sicherungselement aus, das Sie wiederherstellen möchten.

   Wenn Sie eine virtuelle Maschine auswählen, können Sie die Liste der durchgeführten Sicherungen für diese virtuelle Maschine sehen.
5. Klicken Sie auf **Wiederherstellen** zum Starten des Assistenten zum Wiederherstellen von Sicherungen.
6. Prüfen Sie auf der Seite zum Auswählen der Sicherung, ob die Liste der Sicherungen korrekt ist, entfernen Sie die Sicherungen, die nicht für die Wiederherstellung verwendet werden sollen, und klicken Sie auf **Weiter**.
7. Auf der Seite „Wiederherstellungsoption einstellen“ muss das Kontrollkästchen **Am ursprünglichen Speicherort wiederherstellen** aktiviert bleiben.

   Wichtig Wenn die virtuelle Festplatte der ursprünglichen virtuellen Maschine entfernt oder gelöscht wurde, können Sie die virtuelle Maschine nicht an ihrem Ursprungsstandort wiederherstellen. Die VMDK muss an einem neuen Speicherort wiederhergestellt werden.

   ---
8. (Optional) Wählen Sie unter **Erweiterte Optionen** einen neuen Datenspeicher zum Einschalten der virtuellen Maschine nach der Wiederherstellung und zum Neuverbinden der Netzwerkkarte aus.
9. Klicken Sie auf **Weiter**.

10 Überprüfen Sie auf der Seite „Bereit zum Abschließen“ die Übersicht zu Ihren Wiederherstellungsanforderungen und klicken Sie auf **Beenden**, um die Wiederherstellung zu starten.

HINWEIS Wenn Sie in Schritt 8 die Neuverbindung der Netzwerkkarte während der Wiederherstellung ausgewählt haben, stellen Sie sicher, dass die Netzwerkkonfiguration für die neu erstellte virtuelle Maschine korrekt ist. Die neue VM-Netzwerkkarte verwendet möglicherweise dieselbe IP-Adresse wie die ursprüngliche virtuelle Maschine, was Konflikte verursacht.

In einem Dialogfeld wird bestätigt, dass der Wiederherstellungsvorgang erfolgreich initiiert wurde. Sie können den Wiederherstellungsfortschritt im Bereich „Kürzlich bearbeitete Aufgaben“ überwachen.

Wiederherstellen einer virtuellen Maschine an einem neuen Speicherort

Sie können vollständige Image-Sicherungen manuell mit dem Assistenten zum Wiederherstellen von Sicherungen wiederherstellen.

Voraussetzungen

- Stellen Sie die vSphere Data Protection-Appliance bereit und konfigurieren Sie sie.
- Sichern Sie eine virtuelle Maschine, auf der vCenter Server, vCenter Server Appliance oder Platform Services Controller ausgeführt wird. Siehe „Erstellen einer Sicherungsaufgabe in vSphere Data Protection“, auf Seite 287.
- Verwenden Sie den vSphere Web Client zum Anmelden bei der vCenter Server-Instanz, die Ihre Umgebung verwaltet. Melden Sie sich als der Benutzer mit Administratorrechten an, der während der Konfiguration von vSphere Data Protection verwendet wurde.
- Stellen Sie sicher, dass die virtuelle Maschine, die Sie wiederherstellen möchten, ausgeschaltet ist.

Vorgehensweise

1 Klicken Sie auf der Startseite von vSphere Web Client auf **vSphere Data Protection**.

2 Klicken Sie auf die Registerkarte **Wiederherstellen**.

3 (Optional) Filtern Sie die Sicherungen zum Verfeinern Ihrer Suche.

4 Wählen Sie eine virtuelle Maschine in der Spalte „Name“ und dann mindestens ein Sicherungselement aus, das Sie wiederherstellen möchten.

Wenn Sie eine virtuelle Maschine auswählen, können Sie die Liste der durchgeführten Sicherungen für diese virtuelle Maschine sehen.

5 Klicken Sie auf **Wiederherstellen** zum Starten des Assistenten zum Wiederherstellen von Sicherungen.

6 Prüfen Sie auf der Seite zum Auswählen der Sicherung, ob die Liste der Sicherungen korrekt ist, entfernen Sie die Sicherungen, die nicht für die Wiederherstellung verwendet werden sollen, und klicken Sie auf **Weiter**.

7 Deaktivieren Sie auf der Seite „Wiederherstellungsoption einstellen“ das Kontrollkästchen **Am ursprünglichen Speicherort wiederherstellen**, um die Wiederherstellungsoptionen für jede Sicherung festzulegen, die Sie an einem neuen Speicherort wiederherstellen.

8 Geben Sie den neuen Namen der virtuellen Maschine ein und klicken Sie auf **Auswählen**, um einen neuen Host für die wiederhergestellte virtuelle Maschine auszuwählen.

9 Wählen Sie den Datenspeicher aus, in dem die virtuelle Maschine wiederhergestellt werden soll, und klicken Sie auf **Weiter**.

10 (Optional) Wählen Sie unter **Erweiterte Optionen** einen neuen Datenspeicher zum Einschalten der virtuellen Maschine nach der Wiederherstellung und zum Neuverbinden der Netzwerkkarte aus.

11 Klicken Sie auf **Weiter**.

12 Überprüfen Sie auf der Seite „Bereit zum Abschließen“ die Übersicht zu Ihren Wiederherstellungsanforderungen und klicken Sie auf **Beenden**, um die Wiederherstellung zu starten.

Hinweis Wenn Sie in Schritt 10 die Neuverbindung der Netzwerkkarte während der Wiederherstellung ausgewählt haben, prüfen Sie die Netzwerkkonfiguration für die neu erstellte virtuelle Maschine. Die neue VM-Netzwerkkarte verwendet möglicherweise dieselbe IP-Adresse wie die ursprüngliche virtuelle Maschine, was Konflikte verursacht.

In einem Dialogfeld wird bestätigt, dass der Wiederherstellungsvorgang erfolgreich initiiert wurde. Sie können den Wiederherstellungsfortschritt im Bereich „Kürzlich bearbeitete Aufgaben“ überwachen.

Wiederherstellen einer virtuellen Maschine mit der Direct-to-Host-Notfallwiederherstellung

Mit der Direct-to-Host-Notfallwiederherstellung können Sie die virtuelle Maschine wiederherstellen, die vCenter Server, vCenter Server Appliance oder Platform Services Controller enthält, wenn vCenter Server nicht mehr verfügbar ist oder wenn Sie nicht über den vSphere Web Client auf die Benutzeroberfläche von vSphere Data Protection zugreifen können.

Viele zentrale Vorgänge von vSphere Data Protection hängen von vCenter Server ab. Wenn vCenter Server nicht mehr verfügbar ist, kann mit einer Notfallwiederherstellung die virtuelle Maschine, die vCenter Server, vCenter Server Appliance oder Platform Services Controller enthält, direkt auf dem ESXi-Host, auf dem die vSphere Data Protection-Appliance ausführt wird, wiederhergestellt werden. Auf der Registerkarte **Notfallwiederherstellung** wird eine Liste der virtuellen Maschinen angezeigt, die durch die vSphere Data Protection-Appliance gesichert wurden. Diese virtuellen Maschinen mit vCenter Server- oder Platform Services Controller-Instanzen können auf dem ESXi-Host, auf dem die vSphere Data Protection-Appliance ausgeführt wird, als neue virtuelle Maschinen wiederhergestellt werden. Informationen zu Best Practices und Einschränkungen zur Notfallwiederherstellung finden Sie in der Dokumentation für *vSphere Data Protection*.

Vorgehensweise

1 Melden Sie sich als Administrator bei vSphere Client an und klicken Sie auf die Registerkarte **Übersicht**.

   a Wählen Sie unter „Hostverwaltung“ die Option **Host von vCenter Server trennen** aus.

   b Klicken Sie auf **Ja** bei der Frage, ob der Host von vCenter Server getrennt werden soll.

2 Navigieren Sie in einem Webbrowser zum Dienstprogramm zum Konfigurieren von vSphere Data Protection.

   https://*ip_address_VDP_Appliance*:8543/vdp-configure/.

3 Wählen Sie auf der Registerkarte **Notfallwiederherstellung** die virtuelle Maschine aus, die als Wiederherstellungspunkt dienen soll, und klicken Sie auf **Wiederherstellen**.

4 Geben Sie im Dialogfeld „Hostanmeldedaten“ gültige Hostanmeldedaten ein und klicken Sie auf **OK**.

5 Geben Sie im Dialogfeld „Wiederherstellen einer Sicherung“ einen neuen Namen ein.

6 Wählen Sie einen Datenspeicher als Ziel für die Sicherung aus und klicken Sie auf **Wiederherstellen**.



Vorsicht Die Kapazität des Datenspeichers ist aufgeführt. Stellen Sie sicher, dass Sie einen Datenspeicher mit genug Festplattenspeicherplatz für die Wiederherstellung auswählen. Bei unzureichendem Speicherplatz schlägt die Wiederherstellung fehl.

7 Prüfen Sie im Bereich „Kürzlich bearbeitete Aufgaben“ den Fortschritt und stellen Sie sicher, dass die Wiederherstellung erfolgreich ausgeführt wird.

HINWEIS Die wiederhergestellte virtuelle Maschine wird in der Bestandsliste auf der vSphere-Hostebene aufgeführt. Die Wiederherstellung in einem speziellen Bestandspfad wird nicht unterstützt.

Sichern und Wiederherstellen von vCenter Server mit eingebettetem Platform Services Controller

Ihre Umgebung besteht möglicherweise aus vCenter Server oder einer vCenter Server Appliance mit eingebettetem Platform Services Controller. Mithilfe von vSphere Data Protection können Sie eine vCenter Server-Umgebung mit eingebettetem Platform Services Controller sichern und wiederherstellen.

WICHTIG Nur virtuelle Maschinen, die vCenter Server, vCenter Server Appliance und Platform Services Controller enthalten, können gesichert und wiederhergestellt werden. Das Sichern und Wiederherstellen von physischen Maschinen, auf denen vCenter Server ausgeführt wird, ist nicht möglich.

Das Sichern und Wiederherstellen einer vCenter Server-Instanz mit eingebettetem Platform Services Controller beinhaltet die folgenden Aufgaben:

1 Stellen Sie die vSphere Data Protection-Appliance bereit.

   Siehe „Bereitstellen der OVF-Vorlage für vSphere Data Protection“, auf Seite 284.

2 Schließen Sie die Erstkonfiguration von vSphere Data Protection ab.

   Siehe „Konfigurieren von vSphere Data Protection“, auf Seite 285.

3 Führen Sie Image-basierte Sicherungen für alle vCenter Server-Instanzen durch.

   Siehe „Erstellen einer Sicherungsaufgabe in vSphere Data Protection“, auf Seite 287.

4 (Optional) Um einen vorhandenen Sicherungsauftrag sofort auszuführen, starten Sie den Vorgang manuell.

   Siehe „Manuelles Starten einer Sicherungsaufgabe“, auf Seite 288.

5 Stellen Sie die fehlgeschlagene vCenter Server-Instanz mithilfe einer der verfügbaren Methoden wieder her:

   - Stellen Sie eine virtuelle Maschine am ursprünglichen Speicherort wieder her.

     Siehe „Wiederherstellen einer virtuellen Maschine am ursprünglichen Speicherort“, auf Seite 289.

   - Stellen Sie eine virtuelle Maschine an einem neuen Speicherort wieder her.

     Siehe „Wiederherstellen einer virtuellen Maschine an einem neuen Speicherort“, auf Seite 290.

   - Stellen Sie eine virtuelle Maschine direkt auf dem ESXi-Host wieder her, auf dem die vSphere Data Protection-Appliance ausgeführt wird, falls der vCenter Server-Dienst nicht mehr verfügbar ist oder falls Sie mit dem vSphere Web Client nicht auf die Benutzeroberfläche von vSphere Data Protection zugreifen können.

     Siehe „Wiederherstellen einer virtuellen Maschine mit der Direct-to-Host-Notfallwiederherstellung“, auf Seite 291.

6 Schalten Sie die virtuelle Maschine ein, die den wiederhergestellten vCenter Server enthält.

Sichern und Wiederherstellen einer vCenter Server -Umgebung mit einem einzelnen externen Platform Services Controller

Ihre Umgebung besteht möglicherweise aus vielen vCenter Server-Instanzen, die bei einem einzigen Platform Services Controller registriert sind. Mithilfe von vSphere Data Protection können Sie eine virtuelle Maschine sichern und wiederherstellen, die einen Platform Services Controller enthält. Sie können auch mithilfe von vSphere Data Protection entweder virtuelle Maschinen, die vCenter Server-Instanzen enthalten, oder aber vCenter Server Appliance-Instanzen, die bei einem einzelnen externen Platform Services Controller registriert sind, sichern und wiederherstellen.

Hinweis Falls vCenter Server- und Platform Services Controller-Instanzen gleichzeitig fehlschlagen, müssen Sie zuerst die Platform Services Controller- und dann die vCenter Server-Instanzen wiederherstellen.

- Sichern und Wiederherstellen von Platform Services Controller auf Seite 293

  Sie können einen Platform Services Controller installieren und bereitstellen sowie mehrere vCenter Server-Instanzen beim selben Platform Services Controller registrieren. Mithilfe von vSphere Data Protection können Sie Ihre Umgebung für den Fall sichern und wiederherstellen, dass der externe Platform Services Controller fehlschlägt.

- Sichern und Wiederherstellen von vCenter Server auf Seite 295

  Sie können einen Platform Services Controller installieren und bereitstellen sowie mehrere vCenter Server-Instanzen beim selben Platform Services Controller registrieren. Mithilfe von vSphere Data Protection können Sie die gesamte Netzwerkumgebung sichern und wiederherstellen, damit Sie beim Ausfall einer vCenter Server-Instanz die fehlgeschlagene vCenter Server-Instanz wiederherstellen können.

Sichern und Wiederherstellen von Platform Services Controller

Sie können einen Platform Services Controller installieren und bereitstellen sowie mehrere vCenter Server-Instanzen beim selben Platform Services Controller registrieren. Mithilfe von vSphere Data Protection können Sie Ihre Umgebung für den Fall sichern und wiederherstellen, dass der externe Platform Services Controller fehlschlägt.

Wichtig Nur virtuelle Maschinen, die vCenter Server, vCenter Server Appliance und Platform Services Controller enthalten, können gesichert und wiederhergestellt werden. Das Sichern und Wiederherstellen von physischen Maschinen, auf denen vCenter Server ausgeführt wird, ist nicht möglich.

---

1. Stellen Sie die vSphere Data Protection-Appliance bereit.

   Siehe „Bereitstellen der OVF-Vorlage für vSphere Data Protection“, auf Seite 284.

2. Schließen Sie die Erstkonfiguration von vSphere Data Protection ab.

   Siehe „Konfigurieren von vSphere Data Protection“, auf Seite 285.

3. Führen Sie Image-basierte Sicherungen für den externen Platform Services Controller und für alle vCenter Server-Instanzen durch.

   Siehe „Erstellen einer Sicherungsaufgabe in vSphere Data Protection“, auf Seite 287.

   Hinweis Sichern Sie alle vCenter Server- und Platform Services Controller-Instanzen gleichzeitig.

   ---

4. (Optional) Um einen vorhandenen Sicherungsauftrag sofort auszuführen, starten Sie den Vorgang manuell.

   Siehe „Manuelles Starten einer Sicherungsaufgabe“, auf Seite 288.

5 Stellen Sie den fehlgeschlagenen Platform Services Controller anhand des Sicherungs-Images mithilfe der Direct-to-Host-Notfallwiederherstellung wieder her.

   Weitere Informationen finden Sie unter „Wiederherstellen einer virtuellen Maschine mit der Direct-to-Host-Notfallwiederherstellung“, auf Seite 291.

6 Schalten Sie die virtuelle Maschine ein, die den Platform Services Controller enthält.

   Wichtig Wenn Sie für unter Windows installierte Platform Services Controller-Instanzen aufgefordert werden, die virtuelle Maschine neu zu starten, sollten Sie die virtuelle Maschine erst nach dem Ausführen des Skripts `psc-restore` neu starten.

7 Melden Sie sich bei der Platform Services Controller-Instanz an.

   - Melden Sie sich für einen als Appliance bereitgestellten Platform Services Controller bei der vCenter Server Appliance-Shell als **`root`** an.
   - Melden Sie sich für einen unter Windows installierten Platform Services Controller als Administrator bei der virtuellen Maschine an, auf der Sie vCenter Server installiert haben.

8 Stellen Sie sicher, dass keine Platform Services Controller-Dienste ausgeführt werden.

   - Für einen als Appliance bereitgestellten Platform Services Controller führen Sie den Befehl `service-control --status --all` in der Appliance-Shell aus.
   - Für einen unter Windows installierten Platform Services Controller wählen Sie im **Start**-Menü von Windows **Systemsteuerung > Verwaltung > Dienste** aus.

9 Führen Sie das Skript `psc-restore` aus, um den Platform Services Controller wiederherzustellen.

Option	Schritte
Für einen als Appliance bereitgestellten Platform Services Controller	Führen Sie das Skript `psc-restore` in der Appliance-Shell aus. `psc-restore -u` *`psc_administrator_username`* `-p` *`psc_administrator_password`* **Hinweis** Wenn Sie keine Argumente angeben, werden Sie dreimal zur Eingabe der erforderlichen Argumente aufgefordert, bevor das Skript geschlossen wird.
Für einen unter Windows installierten Platform Services Controller	1 Navigieren Sie an der Windows-Eingabeaufforderung zum Skript `psc-restore`. Dieses Skript ist standardmäßig unter `C:\Program Files\VMware\vCenter Server\` gespeichert. 2 Führen Sie das Skript `psc-restore` aus. `psc-restore -u` *`psc_administrator_username`* `-p` *`psc_administrator_password`* **Hinweis** Wenn Sie keine Argumente angeben, wird das Skript geschlossen, nachdem Sie darauf hingewiesen wurden, dass die erforderlichen Argumente nicht angegeben wurden.

10 Stellen Sie sicher, dass alle Platform Services Controller-Dienste der wiederhergestellten Platform Services Controller-Instanz ausgeführt werden.

   - Für einen als Appliance bereitgestellten Platform Services Controller führen Sie den Befehl `service-control --status --all` in der Appliance-Shell aus.
   - Für einen unter Windows installierten Platform Services Controller wählen Sie im **Start**-Menü von Windows **Systemsteuerung > Verwaltung > Dienste** aus.

11 Starten Sie alle vCenter Server-Dienste neu.

   Siehe *vCenter Server und Hostverwaltung*.

Sichern und Wiederherstellen von vCenter Server

Sie können einen Platform Services Controller installieren und bereitstellen sowie mehrere vCenter Server-Instanzen beim selben Platform Services Controller registrieren. Mithilfe von vSphere Data Protection können Sie die gesamte Netzwerkumgebung sichern und wiederherstellen, damit Sie beim Ausfall einer vCenter Server-Instanz die fehlgeschlagene vCenter Server-Instanz wiederherstellen können.

WICHTIG Nur virtuelle Maschinen, die vCenter Server, vCenter Server Appliance und Platform Services Controller enthalten, können gesichert und wiederhergestellt werden. Das Sichern und Wiederherstellen von physischen Maschinen, auf denen vCenter Server ausgeführt wird, ist nicht möglich.

---

1 Stellen Sie die vSphere Data Protection-Appliance bereit.

   Siehe „Bereitstellen der OVF-Vorlage für vSphere Data Protection“, auf Seite 284.

2 Schließen Sie die Erstkonfiguration von vSphere Data Protection ab.

   Siehe „Konfigurieren von vSphere Data Protection“, auf Seite 285.

3 Führen Sie Image-basierte Sicherungen für den externen Platform Services Controller und für alle vCenter Server-Instanzen durch.

   Siehe „Erstellen einer Sicherungsaufgabe in vSphere Data Protection“, auf Seite 287.

   HINWEIS Sichern Sie alle vCenter Server- und Platform Services Controller-Instanzen gleichzeitig.

   ---

4 (Optional) Um einen vorhandenen Sicherungsauftrag sofort auszuführen, starten Sie den Vorgang manuell.

   Siehe „Manuelles Starten einer Sicherungsaufgabe“, auf Seite 288.

5 Stellen Sie jeden fehlgeschlagenen vCenter Server wieder her.

   - Stellen Sie eine virtuelle Maschine am ursprünglichen Speicherort wieder her.

     Siehe „Wiederherstellen einer virtuellen Maschine am ursprünglichen Speicherort“, auf Seite 289.

   - Stellen Sie eine virtuelle Maschine an einem neuen Speicherort wieder her.

     Siehe „Wiederherstellen einer virtuellen Maschine an einem neuen Speicherort“, auf Seite 290.

   - Stellen Sie eine virtuelle Maschine direkt auf dem ESXi-Host wieder her, auf dem die vSphere Data Protection-Appliance ausgeführt wird, falls der vCenter Server-Dienst nicht mehr verfügbar ist oder falls Sie mit dem vSphere Web Client nicht auf die Benutzeroberfläche von vSphere Data Protection zugreifen können.

     Siehe „Wiederherstellen einer virtuellen Maschine mit der Direct-to-Host-Notfallwiederherstellung“, auf Seite 291.

6 Schalten Sie die virtuelle Maschine ein, die den wiederhergestellten vCenter Server enthält.

Sichern und Wiederherstellen einer vCenter Server -Umgebung mit mehreren Platform Services Controller -Instanzen

Mithilfe von vSphere Data Protection können Sie eine Umgebung sichern und wiederherstellen, in der die vCenter Server-Instanzen bei verschiedenen Platform Services Controller-Instanzen registriert sind und die Infrastrukturdaten zwischen den Platform Services Controller-Instanzen repliziert werden.

HINWEIS Falls vCenter Server- und Platform Services Controller-Instanzen gleichzeitig fehlschlagen, müssen Sie zuerst die Platform Services Controller- und dann die vCenter Server-Instanzen wiederherstellen.

- Sichern und Wiederherstellen einer einzelnen Platform Services Controller-Instanz auf Seite 296

  Ihre Umgebung enthält möglicherweise mehrere vCenter Server-Instanzen, für die unterschiedliche externe Platform Services Controller-Instanzen registriert sind, deren Daten repliziert werden. Mithilfe von vSphere Data Protection können Sie die gesamte Netzwerkumgebung sichern und wiederherstellen, damit Sie beim Ausfall einer Platform Services Controller-Instanz den fehlgeschlagenen Platform Services Controller wiederherstellen können.

- Sichern und Wiederherstellen mehrerer Platform Services Controller-Instanzen auf Seite 298

  Ihre Umgebung enthält möglicherweise mehrere vCenter Server-Instanzen, für die unterschiedliche externe Platform Services Controller-Instanzen registriert sind, deren Daten repliziert werden. Mithilfe von vSphere Data Protection können Sie die gesamte Netzwerkumgebung sichern und wiederherstellen, damit Sie beim Ausfall mehrerer Platform Services Controller-Instanzen diese wiederherstellen können.

- Sichern und Wiederherstellen aller Platform Services Controller-Instanzen auf Seite 301

  Ihre Umgebung enthält möglicherweise mehrere vCenter Server-Instanzen, für die unterschiedliche externe Platform Services Controller-Instanzen registriert sind, deren Daten repliziert werden. Mithilfe von vSphere Data Protection können Sie die gesamte Netzwerkumgebung sichern und wiederherstellen. Bei einem Ausfall aller Platform Services Controller-Instanzen können Sie die Umgebung wiederherstellen.

- Sichern und Wiederherstellen von vCenter Server auf Seite 305

  Ihre Umgebung enthält möglicherweise mehrere vCenter Server-Instanzen, für die unterschiedliche externe Platform Services Controller-Instanzen registriert sind, und die Infrastrukturdaten werden zwischen den Platform Services Controller-Daten repliziert. Mithilfe von vSphere Data Protection können Sie die gesamte Netzwerkumgebung sichern und wiederherstellen, damit Sie fehlgeschlagene vCenter Server-Instanzen wiederherstellen können.

Sichern und Wiederherstellen einer einzelnen Platform Services Controller - Instanz

Ihre Umgebung enthält möglicherweise mehrere vCenter Server-Instanzen, für die unterschiedliche externe Platform Services Controller-Instanzen registriert sind, deren Daten repliziert werden. Mithilfe von vSphere Data Protection können Sie die gesamte Netzwerkumgebung sichern und wiederherstellen, damit Sie beim Ausfall einer Platform Services Controller-Instanz den fehlgeschlagenen Platform Services Controller wiederherstellen können.

WICHTIG Nur virtuelle Maschinen, die vCenter Server, vCenter Server Appliance und Platform Services Controller enthalten, können gesichert und wiederhergestellt werden. Das Sichern und Wiederherstellen von physischen Maschinen, auf denen vCenter Server ausgeführt wird, ist nicht möglich.

---

1. Stellen Sie die vSphere Data Protection-Appliance bereit.

   Siehe „Bereitstellen der OVF-Vorlage für vSphere Data Protection“, auf Seite 284.

2. Schließen Sie die Erstkonfiguration von vSphere Data Protection ab.

   Siehe „Konfigurieren von vSphere Data Protection“, auf Seite 285.

3. Führen Sie Image-basierte Sicherungen für den externen Platform Services Controller und für alle vCenter Server-Instanzen durch.

   Siehe „Erstellen einer Sicherungsaufgabe in vSphere Data Protection“, auf Seite 287.

   HINWEIS Sichern Sie alle vCenter Server- und Platform Services Controller-Instanzen gleichzeitig.

4. (Optional) Um einen vorhandenen Sicherungsauftrag sofort auszuführen, starten Sie den Vorgang manuell.

Siehe „Manuelles Starten einer Sicherungsaufgabe“, auf Seite 288.

5 Führen Sie einen Neuverweis der Verbindungen zwischen den vCenter Server-Instanzen, die beim Platform Services Controller registriert sind, auf einen verbleibenden funktionsfähigen externen Platform Services Controller durch.

Siehe „Neuverweisen der Verbindungen zwischen vCenter Server und Platform Services Controller“, auf Seite 280.

Wichtig Durch das Neuverweisen der Verbindungen zwischen vCenter Server und dem Platform Services Controller gehen alle Sicherungs- und Replizierungsaufträge verloren. Vorhandene Wiederherstellungspunkte bleiben intakt, aber Sie müssen Sicherungs- und Replizierungsaufträge neu erstellen.

---

6 Stellen Sie den fehlgeschlagenen Platform Services Controller wiederher:

- Stellen Sie eine virtuelle Maschine am ursprünglichen Speicherort wieder her.

  Siehe „Wiederherstellen einer virtuellen Maschine am ursprünglichen Speicherort“, auf Seite 289.

- Stellen Sie eine virtuelle Maschine an einem neuen Speicherort wieder her.

  Siehe „Wiederherstellen einer virtuellen Maschine an einem neuen Speicherort“, auf Seite 290.

- Stellen Sie eine virtuelle Maschine direkt auf dem ESXi-Host wieder her, auf dem die vSphere Data Protection-Appliance ausgeführt wird, falls der vCenter Server-Dienst nicht mehr verfügbar ist oder falls Sie mit dem vSphere Web Client nicht auf die Benutzeroberfläche von vSphere Data Protection zugreifen können.

  Siehe „Wiederherstellen einer virtuellen Maschine mit der Direct-to-Host-Notfallwiederherstellung“, auf Seite 291.

7 Schalten Sie die virtuelle Maschine ein, die den Platform Services Controller enthält.

Wichtig Wenn Sie für unter Windows installierte Platform Services Controller-Instanzen aufgefordert werden, die virtuelle Maschine neu zu starten, sollten Sie die virtuelle Maschine erst nach dem Ausführen des Skripts `psc-restore` neu starten.

---

8 Melden Sie sich bei der Platform Services Controller-Instanz an.

- Melden Sie sich für einen als Appliance bereitgestellten Platform Services Controller bei der vCenter Server Appliance-Shell als **`root`** an.
- Melden Sie sich für einen unter Windows installierten Platform Services Controller als Administrator bei der virtuellen Maschine an, auf der Sie vCenter Server installiert haben.

9 Stellen Sie sicher, dass keine Platform Services Controller-Dienste ausgeführt werden.

- Für einen als Appliance bereitgestellten Platform Services Controller führen Sie den Befehl `service-control --status --all` in der Appliance-Shell aus.
- Für einen unter Windows installierten Platform Services Controller wählen Sie im **Start**-Menü von Windows **Systemsteuerung > Verwaltung > Dienste** aus.

10 Führen Sie das Skript `psc-restore` aus, um den Platform Services Controller wiederherzustellen.

Option	Schritte
Für einen als Appliance bereitgestellten Platform Services Controller	Führen Sie das Skript `psc-restore` in der Appliance-Shell aus. `psc-restore -u` *`psc_administrator_username`* `-p` *`psc_administrator_password`* **Hinweis** Wenn Sie keine Argumente angeben, werden Sie dreimal zur Eingabe der erforderlichen Argumente aufgefordert, bevor das Skript geschlossen wird.
Für einen unter Windows installierten Platform Services Controller	1 Navigieren Sie an der Windows-Eingabeaufforderung zum Skript `psc-restore`. Dieses Skript ist standardmäßig unter `C:\Program Files\VMware\vCenter Server\` gespeichert. 2 Führen Sie das Skript `psc-restore` aus. `psc-restore -u` *`psc_administrator_username`* `-p` *`psc_administrator_password`* **Hinweis** Wenn Sie keine Argumente angeben, wird das Skript geschlossen, nachdem Sie darauf hingewiesen wurden, dass die erforderlichen Argumente nicht angegeben wurden.

11 Stellen Sie sicher, dass alle Platform Services Controller-Dienste der wiederhergestellten Platform Services Controller-Instanz ausgeführt werden.

- Für einen als Appliance bereitgestellten Platform Services Controller führen Sie den Befehl `service-control --status --all` in der Appliance-Shell aus.
- Für einen unter Windows installierten Platform Services Controller wählen Sie im **Start**-Menü von Windows **Systemsteuerung > Verwaltung > Dienste** aus.

12 Verweisen Sie Verbindungen zwischen den vCenter Server-Instanzen erneut auf den wiederhergestellten Platform Services Controller.

Siehe „Neuverweisen der Verbindungen zwischen vCenter Server und Platform Services Controller“, auf Seite 280.

Wichtig Durch das Neuverweisen der Verbindungen zwischen vCenter Server und dem Platform Services Controller gehen alle Sicherungs- und Replizierungsaufträge verloren. Vorhandene Wiederherstellungspunkte bleiben intakt, aber Sie müssen Sicherungs- und Replizierungsaufträge neu erstellen.

Sichern und Wiederherstellen mehrerer Platform Services Controller -Instanzen

Ihre Umgebung enthält möglicherweise mehrere vCenter Server-Instanzen, für die unterschiedliche externe Platform Services Controller-Instanzen registriert sind, deren Daten repliziert werden. Mithilfe von vSphere Data Protection können Sie die gesamte Netzwerkumgebung sichern und wiederherstellen, damit Sie beim Ausfall mehrerer Platform Services Controller-Instanzen diese wiederherstellen können.

Wichtig Nur virtuelle Maschinen, die vCenter Server, vCenter Server Appliance und Platform Services Controller enthalten, können gesichert und wiederhergestellt werden. Das Sichern und Wiederherstellen von physischen Maschinen, auf denen vCenter Server ausgeführt wird, ist nicht möglich.

1 Stellen Sie die vSphere Data Protection-Appliance bereit.

Siehe „Bereitstellen der OVF-Vorlage für vSphere Data Protection“, auf Seite 284.

2 Schließen Sie die Erstkonfiguration von vSphere Data Protection ab.

Siehe „Konfigurieren von vSphere Data Protection“, auf Seite 285.

3 Führen Sie Image-basierte Sicherungen für alle Platform Services Controller- und vCenter Server-Instanzen durch.

Siehe „Erstellen einer Sicherungsaufgabe in vSphere Data Protection“, auf Seite 287.

Hinweis Sichern Sie alle vCenter Server- und Platform Services Controller-Instanzen gleichzeitig.

---

4 (Optional) Um einen vorhandenen Sicherungsauftrag sofort auszuführen, starten Sie den Vorgang manuell.

Siehe „Manuelles Starten einer Sicherungsaufgabe“, auf Seite 288.

5 Rufen Sie die Platform Services Controller-Replizierungstopologie von einem funktionsfähigen Platform Services Controller ab.

Hinweis Der Replizierungstopologiebefehl liefert nur Informationen zu den direkten Replizierungspartnern der funktionsfähigen Platform Services Controller-Instanz.

Option	Schritte
Für einen als Appliance bereitgestellten Platform Services Controller	1 Melden Sie sich bei der Appliance-Shell als Root-Benutzer an. ■ Wenn Sie direkten Zugriff auf die Appliance-Konsole haben, drücken Sie Alt+F1. ■ Wenn Sie eine Remoteverbindung herstellen möchten, verwenden Sie SSH oder eine andere Remotekonsolenverbindung, um eine Sitzung mit der Appliance zu starten. 2 (Optional) Aktivieren Sie die Bash-Shell. `shell.set --enabled true` 3 Führen Sie `shell` aus, um auf die Bash-Shell zuzugreifen. 4 Führen Sie den Befehl `vdcrepadmin` aus. `/usr/lib/vmware-vmdir/bin/vdcrepadmin -f showpartners -h localhost -u` *`PSC_Administrator_username`* `-w` *`PSC_Administrator_password`*
Für einen unter Windows installierten Platform Services Controller	1 Melden Sie sich als Administrator an der Windows-Maschine an. 2 Führen Sie an der Windows-Eingabeaufforderung den Befehl `vdcrepadmin` aus. `C:\Program Files\VMware\vCenter Server\vmdird\bin\vdcrepadmin -f showpartners -h localhost -u` *`psc_administrator_username`* `-w` *`psc_administrator_password`*

6 (Optional) Wenn eine vCenter Server-Instanz bei einem fehlgeschlagenen Platform Services Controller registriert ist, verweisen Sie die Verbindungen zwischen den vCenter Server-Instanzen und den fehlgeschlagenen Platform Services Controller-Instanzen erneut auf einen verbleibenden und funktionsfähigen externen Platform Services Controller.

Siehe „Neuverweisen der Verbindungen zwischen vCenter Server und Platform Services Controller“, auf Seite 280.

Wichtig Durch das Neuverweisen der Verbindungen zwischen vCenter Server und dem Platform Services Controller gehen alle Sicherungs- und Replizierungsaufträge verloren. Vorhandene Wiederherstellungspunkte bleiben intakt, aber Sie müssen Sicherungs- und Replizierungsaufträge neu erstellen.

---

7 Stellen Sie die Replizierungspartner einer funktionsfähigen Platform Services Controller-Instanz wiederher.

   a Stellen Sie einen fehlgeschlagenen Platform Services Controller anhand des Sicherungs-Images wiederher.

      - Stellen Sie eine virtuelle Maschine am ursprünglichen Speicherort wieder her.

        Siehe „Wiederherstellen einer virtuellen Maschine am ursprünglichen Speicherort“, auf Seite 289.

      - Stellen Sie eine virtuelle Maschine an einem neuen Speicherort wieder her.

        Siehe „Wiederherstellen einer virtuellen Maschine an einem neuen Speicherort“, auf Seite 290.

      - Stellen Sie eine virtuelle Maschine direkt auf dem ESXi-Host wieder her, auf dem die vSphere Data Protection-Appliance ausgeführt wird, falls der vCenter Server-Dienst nicht mehr verfügbar ist oder falls Sie mit dem vSphere Web Client nicht auf die Benutzeroberfläche von vSphere Data Protection zugreifen können.

        Siehe „Wiederherstellen einer virtuellen Maschine mit der Direct-to-Host-Notfallwiederherstellung“, auf Seite 291.

   b Schalten Sie die virtuelle Maschine ein, die den Platform Services Controller enthält.

   WICHTIG Wenn Sie für unter Windows installierte Platform Services Controller-Instanzen aufgefordert werden, die virtuelle Maschine neu zu starten, sollten Sie die virtuelle Maschine erst nach dem Ausführen des Skripts `psc-restore` neu starten.

   c Melden Sie sich bei der Platform Services Controller-Instanz an.

      - Melden Sie sich für einen als Appliance bereitgestellten Platform Services Controller bei der vCenter Server Appliance-Shell als **`root`** an.
      - Melden Sie sich für einen unter Windows installierten Platform Services Controller als Administrator bei der virtuellen Maschine an, auf der Sie vCenter Server installiert haben.

   d Stellen Sie sicher, dass keine Platform Services Controller-Dienste ausgeführt werden.

      - Für einen als Appliance bereitgestellten Platform Services Controller führen Sie den Befehl `service-control --status --all` in der Appliance-Shell aus.
      - Für einen unter Windows installierten Platform Services Controller wählen Sie im **Start**-Menü von Windows **Systemsteuerung > Verwaltung > Dienste** aus.

e Führen Sie das Skript `psc-restore` aus, um den Platform Services Controller wiederherzustellen.

Option	Schritte
Für einen als Appliance bereitgestellten Platform Services Controller	Führen Sie das Skript `psc-restore` in der Appliance-Shell aus. `psc-restore -u` *`psc_administrator_username`* `-p` *`psc_administrator_password`* **Hinweis** Wenn Sie keine Argumente angeben, werden Sie dreimal zur Eingabe der erforderlichen Argumente aufgefordert, bevor das Skript geschlossen wird.
Für einen unter Windows installierten Platform Services Controller	1 Navigieren Sie an der Windows-Eingabeaufforderung zum Skript `psc-restore`. Dieses Skript ist standardmäßig unter `C:\Program Files\VMware\vCenter Server\` gespeichert. 2 Führen Sie das Skript `psc-restore` aus. `psc-restore -u` *`psc_administrator_username`* `-p` *`psc_administrator_password`* **Hinweis** Wenn Sie keine Argumente angeben, wird das Skript geschlossen, nachdem Sie darauf hingewiesen wurden, dass die erforderlichen Argumente nicht angegeben wurden.

8 Stellen Sie sicher, dass alle Platform Services Controller-Dienste der wiederhergestellten Platform Services Controller-Instanz ausgeführt werden.

- Für einen als Appliance bereitgestellten Platform Services Controller führen Sie den Befehl `service-control --status --all` in der Appliance-Shell aus.
- Für einen unter Windows installierten Platform Services Controller wählen Sie im **Start**-Menü von Windows **Systemsteuerung > Verwaltung > Dienste** aus.

9 Wiederholen Sie Listenelement. bis Listenelement., um die Replizierungspartner jeder fehlgeschlagenen Platform Services Controller-Instanz, die Sie wiederhergestellt haben, wiederherzustellen.

Hinweis Stellen Sie zunächst die Platform Services Controller-Instanzen wieder her, die mindestens einen funktionsfähigen Replizierungspartner aufweisen.

10 (Optional) Verweisen Sie Verbindungen zwischen den vCenter Server-Instanzen erneut auf die wiederhergestellten Platform Services Controller-Instanzen, die zuvor unter Listenelement. neu verwiesen wurden, und starten Sie die entsprechenden vCenter Server-Instanzen neu.

Sichern und Wiederherstellen aller Platform Services Controller -Instanzen

Ihre Umgebung enthält möglicherweise mehrere vCenter Server-Instanzen, für die unterschiedliche externe Platform Services Controller-Instanzen registriert sind, deren Daten repliziert werden. Mithilfe von vSphere Data Protection können Sie die gesamte Netzwerkumgebung sichern und wiederherstellen. Bei einem Ausfall aller Platform Services Controller-Instanzen können Sie die Umgebung wiederherstellen.

Wichtig Nur virtuelle Maschinen, die vCenter Server, vCenter Server Appliance und Platform Services Controller enthalten, können gesichert und wiederhergestellt werden. Das Sichern und Wiederherstellen von physischen Maschinen, auf denen vCenter Server ausgeführt wird, ist nicht möglich.

1 Stellen Sie die vSphere Data Protection-Appliance bereit.

Siehe „Bereitstellen der OVF-Vorlage für vSphere Data Protection“, auf Seite 284.

2 Schließen Sie die Erstkonfiguration von vSphere Data Protection ab.

Siehe „Konfigurieren von vSphere Data Protection“, auf Seite 285.

3 Führen Sie Image-basierte Sicherungen für alle Platform Services Controller- und vCenter Server-Instanzen durch.

Siehe „Erstellen einer Sicherungsaufgabe in vSphere Data Protection“, auf Seite 287.

HINWEIS Sichern Sie alle vCenter Server- und Platform Services Controller-Instanzen gleichzeitig.

---

4 (Optional) Um einen vorhandenen Sicherungsauftrag sofort auszuführen, starten Sie den Vorgang manuell.

Siehe „Manuelles Starten einer Sicherungsaufgabe“, auf Seite 288.

5 Stellen Sie die zuletzt gesicherte Platform Services Controller-Instanz mithilfe der Direct-to-Host-Notfallwiederherstellung wiederher.

Siehe „Wiederherstellen einer virtuellen Maschine mit der Direct-to-Host-Notfallwiederherstellung“, auf Seite 291.

6 Schalten Sie die virtuelle Maschine ein, die den Platform Services Controller enthält.

WICHTIG Wenn Sie für unter Windows installierte Platform Services Controller-Instanzen aufgefordert werden, die virtuelle Maschine neu zu starten, sollten Sie die virtuelle Maschine erst nach dem Ausführen des Skripts `psc-restore` neu starten.

---

7 Melden Sie sich bei der Platform Services Controller-Instanz an.

- Melden Sie sich für einen als Appliance bereitgestellten Platform Services Controller bei der vCenter Server Appliance-Shell als **`root`** an.
- Melden Sie sich für einen unter Windows installierten Platform Services Controller als Administrator bei der virtuellen Maschine an, auf der Sie vCenter Server installiert haben.

8 Stellen Sie sicher, dass keine Platform Services Controller-Dienste ausgeführt werden.

- Für einen als Appliance bereitgestellten Platform Services Controller führen Sie den Befehl `service-control --status --all` in der Appliance-Shell aus.
- Für einen unter Windows installierten Platform Services Controller wählen Sie im **Start**-Menü von Windows **Systemsteuerung > Verwaltung > Dienste** aus.

9 Führen Sie das Skript `psc-restore` aus.

Option	Schritte
Für einen als Appliance bereitgestellten Platform Services Controller	Führen Sie das Skript `psc-restore` aus. `psc-restore -u` *`root`* `-p` *`password`* `--ignore-sync`
Für einen unter Windows installierten Platform Services Controller	1 Navigieren Sie an der Windows-Eingabeaufforderung zum Skript `psc-restore`. Dieses Skript ist standardmäßig unter `C:\Program Files\VMware\vCenter Server\` gespeichert. 2 Führen Sie das Skript `psc-restore` aus. `psc-restore -u` *`administrator`* `-p` *`administrator-password`* `--ignore-sync`

10 Rufen Sie nach Abschluss der Wiederherstellung die Platform Services Controller-Replizierungstopologie von einem funktionsfähigen Platform Services Controller ab.

Hinweis Der Replizierungstopologiebefehl liefert nur Informationen zu den direkten Replizierungspartnern der funktionsfähigen Platform Services Controller-Instanz.

Option	Schritte
Für einen als Appliance bereitgestellten Platform Services Controller	1 (Optional) Aktivieren Sie die Bash-Shell. `shell.set --enabled true` 2 Führen Sie `shell` aus, um auf die Bash-Shell zuzugreifen. 3 Führen Sie den Befehl aus, um die Verbundtopologie abzurufen. `/usr/lib/vmware-vmdir/bin/vdcrepadmin -f showpartners -h localhost -u` *`PSC_administrator_username`* `-w` *`PSC_administrator_password`*
Für einen unter Windows installierten Platform Services Controller	1 Melden Sie sich als Administrator an der Windows-Maschine an. 2 Führen Sie an der Windows-Eingabeaufforderung den Befehl zum Abrufen der Verbundtopologie aus. `C:\Program Files\VMware\vCenter Server\vmdird\bin\vdcrepadmin -f showpartners -h localhost -u` *`psc_administrator_username`* `-w` *`psc_administrator_password`*

11 Stellen Sie einen fehlgeschlagenen Replizierungspartner der wiederhergestellten Platform Services Controller-Instanz mithilfe einer der verfügbaren Methoden wiederher:

- Stellen Sie eine virtuelle Maschine am ursprünglichen Speicherort wieder her.

  Siehe „Wiederherstellen einer virtuellen Maschine am ursprünglichen Speicherort“, auf Seite 289.

- Stellen Sie eine virtuelle Maschine an einem neuen Speicherort wieder her.

  Siehe „Wiederherstellen einer virtuellen Maschine an einem neuen Speicherort“, auf Seite 290.

- Stellen Sie eine virtuelle Maschine direkt auf dem ESXi-Host wieder her, auf dem die vSphere Data Protection-Appliance ausgeführt wird, falls der vCenter Server-Dienst nicht mehr verfügbar ist oder falls Sie mit dem vSphere Web Client nicht auf die Benutzeroberfläche von vSphere Data Protection zugreifen können.

  Siehe „Wiederherstellen einer virtuellen Maschine mit der Direct-to-Host-Notfallwiederherstellung“, auf Seite 291.

12 Schalten Sie die virtuelle Maschine ein, die den Platform Services Controller enthält.

Wichtig Wenn Sie für unter Windows installierte Platform Services Controller-Instanzen aufgefordert werden, die virtuelle Maschine neu zu starten, sollten Sie die virtuelle Maschine erst nach dem Ausführen des Skripts `psc-restore` neu starten.

13 Melden Sie sich bei der Platform Services Controller-Instanz an.

- Melden Sie sich für einen als Appliance bereitgestellten Platform Services Controller bei der vCenter Server Appliance-Shell als **`root`** an.
- Melden Sie sich für einen unter Windows installierten Platform Services Controller als Administrator bei der virtuellen Maschine an, auf der Sie vCenter Server installiert haben.

14 Stellen Sie sicher, dass keine Platform Services Controller-Dienste ausgeführt werden.

- Für einen als Appliance bereitgestellten Platform Services Controller führen Sie den Befehl `service-control --status --all` in der Appliance-Shell aus.
- Für einen unter Windows installierten Platform Services Controller wählen Sie im **Start**-Menü von Windows **Systemsteuerung > Verwaltung > Dienste** aus.

15 Führen Sie das Skript `psc-restore` aus, um den Platform Services Controller wiederherzustellen.

Option	Schritte
Für einen als Appliance bereitgestellten Platform Services Controller	Führen Sie das Skript `psc-restore` in der Appliance-Shell aus. `psc-restore -u` *`psc_administrator_username`* `-p` *`psc_administrator_password`* **Hinweis** Wenn Sie keine Argumente angeben, werden Sie dreimal zur Eingabe der erforderlichen Argumente aufgefordert, bevor das Skript geschlossen wird.
Für einen unter Windows installierten Platform Services Controller	1 Navigieren Sie an der Windows-Eingabeaufforderung zum Skript `psc-restore`. Dieses Skript ist standardmäßig unter `C:\Program Files\VMware\vCenter Server\` gespeichert. 2 Führen Sie das Skript `psc-restore` aus. `psc-restore -u` *`psc_administrator_username`* `-p` *`psc_administrator_password`* **Hinweis** Wenn Sie keine Argumente angeben, wird das Skript geschlossen, nachdem Sie darauf hingewiesen wurden, dass die erforderlichen Argumente nicht angegeben wurden.

16 Stellen Sie sicher, dass alle Platform Services Controller-Dienste der wiederhergestellten Platform Services Controller-Instanz ausgeführt werden.

- Für einen als Appliance bereitgestellten Platform Services Controller führen Sie den Befehl `service-control --status --all` in der Appliance-Shell aus.
- Für einen unter Windows installierten Platform Services Controller wählen Sie im **Start**-Menü von Windows **Systemsteuerung > Verwaltung > Dienste** aus.

17 Wiederholen Sie Listenelement. bis Listenelement., um die Replizierungspartner jeder fehlgeschlagenen Platform Services Controller-Instanz, die Sie wiederhergestellt haben, wiederherzustellen.

Hinweis Stellen Sie zunächst die Platform Services Controller-Instanzen wieder her, die mindestens einen funktionsfähigen Replizierungspartner aufweisen.

18 Starten Sie alle vCenter Server-Dienste neu.

Siehe *vCenter Server und Hostverwaltung*.

Sichern und Wiederherstellen von vCenter Server

Ihre Umgebung enthält möglicherweise mehrere vCenter Server-Instanzen, für die unterschiedliche externe Platform Services Controller-Instanzen registriert sind, und die Infrastrukturdaten werden zwischen den Platform Services Controller-Daten repliziert. Mithilfe von vSphere Data Protection können Sie die gesamte Netzwerkumgebung sichern und wiederherstellen, damit Sie fehlgeschlagene vCenter Server-Instanzen wiederherstellen können.

Wichtig Nur virtuelle Maschinen, die vCenter Server, vCenter Server Appliance und Platform Services Controller enthalten, können gesichert und wiederhergestellt werden. Das Sichern und Wiederherstellen von physischen Maschinen, auf denen vCenter Server ausgeführt wird, ist nicht möglich.

---

1. Stellen Sie die vSphere Data Protection-Appliance bereit.

   Siehe „Bereitstellen der OVF-Vorlage für vSphere Data Protection“, auf Seite 284.

2. Schließen Sie die Erstkonfiguration von vSphere Data Protection ab.

   Siehe „Konfigurieren von vSphere Data Protection“, auf Seite 285.

3. Führen Sie Image-basierte Sicherungen für alle Platform Services Controller- und vCenter Server-Instanzen durch.

   Siehe „Erstellen einer Sicherungsaufgabe in vSphere Data Protection“, auf Seite 287.

   Hinweis Sichern Sie alle vCenter Server- und Platform Services Controller-Instanzen gleichzeitig.

   ---

4. (Optional) Um einen vorhandenen Sicherungsauftrag sofort auszuführen, starten Sie den Vorgang manuell.

   Siehe „Manuelles Starten einer Sicherungsaufgabe“, auf Seite 288.

5. Stellen Sie jeden fehlgeschlagenen vCenter Server wieder her.

   - Stellen Sie eine virtuelle Maschine am ursprünglichen Speicherort wieder her.

     Siehe „Wiederherstellen einer virtuellen Maschine am ursprünglichen Speicherort“, auf Seite 289.

   - Stellen Sie eine virtuelle Maschine an einem neuen Speicherort wieder her.

     Siehe „Wiederherstellen einer virtuellen Maschine an einem neuen Speicherort“, auf Seite 290.

   - Stellen Sie eine virtuelle Maschine direkt auf dem ESXi-Host wieder her, auf dem die vSphere Data Protection-Appliance ausgeführt wird, falls der vCenter Server-Dienst nicht mehr verfügbar ist oder falls Sie mit dem vSphere Web Client nicht auf die Benutzeroberfläche von vSphere Data Protection zugreifen können.

     Siehe „Wiederherstellen einer virtuellen Maschine mit der Direct-to-Host-Notfallwiederherstellung“, auf Seite 291.

6. Schalten Sie die virtuelle Maschine ein, die den wiederhergestellten vCenter Server enthält.

Index

O

P

R

S

T

U

V

W

Z